Graduate Texts in Mathematics

Derek J.S. Robinson

A Course in the Theory of Groups

Second Edition

Springer

Graduate Texts in Mathematics 80

Springer Science+Business Media, LLC

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces.
4 HILTON/STAMMBACH. A Course in Homological Algebra.
5 MAC LANE. Categories for the Working Mathematician.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 WERMER. Banach Algebras and Several Complex Variables. 2nd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.

continued after index

Derek J.S. Robinson

A Course in the Theory of Groups

Second Edition

With 40 Illustrations

Springer

Derek J.S. Robinson
Department of Mathematics
University of Illinois at
Urbana-Champaign
Urbana, IL 61801
USA

Mathematics Subject Classification (1991): 20-01

Library of Congress Cataloging-in-Publication Data
Robinson, Derek John Scott.
A course in the theory of groups / Derek J.S. Robinson. — 2nd ed.
p. cm. — (Graduate texts in mathematics ; 80)
Includes bibliographical references (p. –) and index.
ISBN 978-1-4612-6443-9 ISBN 978-1-4419-8594-1 (eBook)
DOI 10.1007/978-1-4419-8594-1
1. Group theory. I. Title. II. Series.
QA174.2.R63 1995
512'.2—dc20 95-4025

Printed on acid-free paper.

Production coordinated by Brian Howe and managed by Bill Imbornoni; manufacturing supervised by Jeffrey Taub.
Typeset by Asco Trade Typesetting Ltd., Hong Kong.

9 8 7 6 5 4 3 2

ISBN 978-1-4612-6443-9

For Judith

Preface to the Second Edition

In preparing this new edition I have tried to keep the changes to a minimum, on the principle that one should not meddle with a relatively successful text. Thus the general form of the book remains the same. Naturally I have taken the opportunity to correct the errors of which I was aware. Also the text has been updated at various points, some proofs have been improved, and lastly about thirty additional exercises are included.

There are three main additions to the book. In the chapter on group extensions an exposition of Schreier's concrete approach via factor sets is given *before* the introduction of covering groups. This seemed to be desirable on pedagogical grounds. Then S. Thomas's elegant proof of the automorphism tower theorem is included in the section on complete groups. Finally an elementary counterexample to the Burnside problem due to N.D. Gupta has been added in the chapter on finiteness properties.

I am happy to have this opportunity to thank the many friends and colleagues who wrote to me about the first edition with comments, suggestions and lists of errors. Their efforts have surely led to an improvement in the text. In particular I thank J.C. Beidleman, F.B. Cannonito, H. Heineken, L.C. Kappe, W. Möhres, R. Schmidt, H. Snevily, B.A.F. Wehrfritz, and J. Wiegold. My thanks are due to Yu Fen Wu for assistance with the proofreading. I also thank Tom von Foerster of Springer-Verlag for making this new edition possible, and for his assistance throughout the project.

University of Illinois at Urbana-Champaign, Derek Robinson
Urbana, Illinois

Preface to the First Edition

"A group is defined by means of the laws of combinations of its symbols," according to a celebrated dictum of Cayley. And this is probably still as good a one-line explanation as any. The concept of a group is surely one of the central ideas of mathematics. Certainly there are few branches of that science in which groups are not employed implicitly or explicitly. Nor is the use of groups confined to pure mathematics. Quantum theory, molecular and atomic structure, and crystallography are just a few of the areas of science in which the idea of a group as a measure of symmetry has played an important part.

The theory of groups is the oldest branch of modern algebra. Its origins are to be found in the work of Joseph Louis Lagrange (1736–1813), Paulo Ruffini (1765–1822), and Évariste Galois (1811–1832) on the theory of algebraic equations. Their groups consisted of permutations of the variables or of the roots of polynomials, and indeed for much of the nineteenth century all groups were finite permutation groups. Nevertheless many of the fundamental ideas of group theory were introduced by these early workers and their successors, Augustin Louis Cauchy (1789–1857), Ludwig Sylow (1832–1918), Camille Jordan (1838–1922) among others.

The concept of an abstract group is clearly recognizable in the work of Arthur Cayley (1821–1895), but it did not really win widespread acceptance until Walther von Dyck (1856–1934) introduced presentations of groups.

The stimulus to study infinite groups came from geometry and topology, the influence of Felix Klein (1849–1925), Sophus Lie (1842–1899), Henri Poincaré (1854–1912), and Max Dehn (1878–1952) being paramount. Thereafter the standard of infinite group theory was borne almost single-handed by Otto Juljevič Schmidt (1891–1956) until the establishment of the Russian school headed by Alexander Gennadievič Kuroš (1908–1971).

In the meantime the first great age of finite group theory had reached its climax in the period immediately before the First World War with the work of Georg Frobenius (1849–1917), William Burnside (1852–1927), and Issai Schur (1875–1936). After 1928, decisive new contributions were made by Philip Hall (1904–1982), Helmut Wielandt, and, in the field of group representations, Richard Dagobert Brauer (1901–1977). The subsequent intense interest in the classification of finite simple groups is very largely the legacy of their work.

This book is intended as an introduction to the general theory of groups. Its aim is to make the reader aware of some of the main accomplishments of group theory, while at the same time providing a reasonable coverage of basic material. The book is addressed primarily to the student who wishes to learn the subject, but it is hoped that it will also prove useful to specialists in other areas as a work of reference.

An attempt has been made to strike a balance between the different branches of group theory, abelian groups, finite groups, infinite groups, and to stress the unity of the subject. In choice of material I have been guided by its inherent interest, accessibility, and connections with other topics. No book of this type can be comprehensive, but I hope it will serve as an introduction to the several excellent research level texts now in print.

The reader is expected to have at least the knowledge and maturity of a graduate student who has completed the first year of study at a North American university or of a first year research student in the United Kingdom. He or she should be familiar with the more elementary facts about rings, fields, and modules, possess a sound knowledge of linear algebra, and be able to use Zorn's Lemma and transfinite induction. However, no knowledge of homological algebra is assumed: those homological methods required in the study of group extensions are introduced as they become necessary. This said, the theory of groups is developed from scratch. Many readers may therefore wish to skip certain sections of Chapters 1 and 2 or to regard them as a review.

A word about the exercises, of which there are some 650. They are to be found at the end of each section and must be regarded as an integral part of the text. Anyone who aspires to master the material should set out to solve as many exercises as possible. They vary from routine tests of comprehension of definitions and theorems to more challenging problems, some theorems in their own right. Exercises marked with an asterisk are referred to at some subsequent point in the text.

Notation is by-and-large standard, and an attempt has been made to keep it to a minimum. At the risk of some unpopularity, I have chosen to write all functions on the right. A list of commonly used symbols is placed at the beginning of the book.

While engaged on this project I enjoyed the hospitality and benefited from the assistance of several institutions: the University of Illinois at

Urbana-Champaign, the University of Warwick, Notre Dame University, and the University of Freiburg. To all of these and to the National Science Foundation I express my gratitude. I am grateful to my friends John Rose and Ralph Strebel who read several chapters and made valuable comments on them. It has been a pleasure to cooperate with Springer-Verlag in this venture and I thank them for their unfailing courtesy and patience.

Contents

Notation

$G, H, \ldots$	Sets, groups, rings, etc.
$\mathfrak{X}, \mathfrak{Y}, \ldots$	Classes of groups
$\alpha, \beta, \gamma, \ldots$	Functions
$x, y, z, \ldots$	Elements of a set
$x\alpha$ or x^α	Image of x under α
x^y	$y^{-1}xy$
$[x, y]$	$x^{-1}y^{-1}xy$
$H \simeq G$	H is isomorphic with G
$H \leq G, H < G$	H is a subgroup, a proper subgroup of the group G.
$H \lhd G$	H is a normal subgroup of G
H sn G	H is a subnormal subgroup of G
$H_1 H_2 \cdots H_n$	Product of subsets of a group
$\langle X_\lambda \mid \lambda \in \Lambda \rangle$	Subgroup generated by subsets X_λ of a group
$\langle X \mid R \rangle$	Group presented by generators X and relators R
$d(G)$	Minimum number of generators of G
$r_p(G), r_0(G), r(G)$	p-rank, torsion-free rank, (Prüfer) rank of G

G^n, nG	Subgroup generated by all g^n or ng where $g \in G$
$G[n]$	Subgroup generated by all $g \in G$ such that $g^n = 1$ or $ng = 0$.
$\lvert S\rvert$	Cardinality of the set S
$\lvert G:H\rvert$	Index of the subgroup H in the group G
$\lvert x\rvert$	Order of the group element x
$C_G(H)$, $N_G(H)$	Centralizer, normalizer of H in G
H^G, H_G	Normal closure, core of H in G
Aut G, Inn G	Automorphism group, inner automorphism group of G
Out G	Aut G/Inn G, outer automorphism group of G
Hol G	Holomorph of G
$\mathrm{Hom}_\Omega(G, H)$	Set of Ω-homomorphisms from G to H
$\mathrm{End}_\Omega\, G$	Set of Ω-endomorphisms of G
$H_1 \times \cdots \times H_n$, $H_1 \oplus \cdots \oplus H_n$, $\underset{\lambda \in \Lambda}{\mathrm{Dr}}\, H_\lambda$	Set product, direct products, direct sums
$H \ltimes N$, $N \rtimes H$	Semidirect products
$\underset{\lambda \in \Lambda}{\mathrm{Cr}}\, H_\lambda$	Cartesian product, Cartesian sum
$H \wr K$	Wreath product
$H_1 * \cdots * H_n$, $\underset{\lambda \in \Lambda}{\mathrm{Fr}}\, H_\lambda$	Free products
$H \otimes K$	Tensor product
$G' = [G, G]$	Derived subgroup of a group G
G_{ab}	G/G'
$G^{(\alpha)}$	Term of the derived series of G
$\gamma_\alpha G$, $\zeta_\alpha G$	Terms of the lower central series, the upper central series of G
ζG	Center of G
Fit G	Fitting subgroup of G
Frat G	Frattini subgroup of G

$M(G)$	Schur multiplicator of G
$O_\pi(G)$	Maximal normal π-subgroup of G
$l_\pi(G)$	π-length of G
$\mathrm{St}_G(X)$, X_G	Stabilizer of X in G
Sym X	Symmetric group on X
S_n, A_n	Symmetric, alternating groups of degree n
D_n	Dihedral group of order n
Q_{2^n}	Generalized quaternion group of order 2^n
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	Sets of integers, rational numbers, real numbers, complex numbers
$\mathbb{Z}_n$	$\mathbb{Z}/n\mathbb{Z}$
R^*	Group of units of a ring R with identity
RG	Group ring of a group G over a ring R with identity element
I_G, $\bar{I}_G$	Augmentation ideals
$\mathrm{GL}(V)$	Group of nonsingular linear transformations of a vector space V
$\mathrm{GL}(n, R)$, $\mathrm{SL}(n, R)$	General linear and special linear groups
$\mathrm{PGL}(n, R)$, $\mathrm{PSL}(n, R)$	Projective general linear and projective special linear groups
$T(n, R)$, $U(n, R)$	Groups of triangular, unitriangular matrices
$B(n, e)$	Free Burnside group with n generators and exponent e
M^G, χ^G	Induced module, induced character
max, min	Maximal, minimal conditions
E_{ij}	Matrix with (i, j) entry 1 and other entries 0.

CHAPTER 1

Fundamental Concepts of Group Theory

In this first chapter we introduce the basic concepts of group theory, developing fairly rapidly the elementary properties that will be familiar to most readers.

1.1. Binary Operations, Semigroups, and Groups

A binary operation on a set is a rule for combining two elements of the set. More precisely, if S is a nonempty set, a *binary operation* on S is a function $\alpha: S \times S \to S$. Thus α associates with each ordered pair (x, y) of elements of S an element $(x, y)\alpha$ of S. It is better notation to write $x \circ y$ for $(x, y)\alpha$, referring to "$\circ$" as the binary operation.

If $\circ$ is *associative*, that is, if:

(i) $(x \circ y) \circ z = x \circ (y \circ z)$ is valid for all x, y, z in S,

then the pair $(S, \circ)$ is called a *semigroup*.

Here we are concerned with a very special type of semigroup. A semigroup $(G, \circ)$ is called a *group* if it has the following properties:

(ii) There exists in G an element e, called a *right identity*, such that $x \circ e = x$ for all x in G.

(iii) To each element x of G there corresponds an element y of G, called a *right inverse* of x, such that $x \circ y = e$.

While it is clear how to define left identity and left inverse, the existence of such elements is not presupposed; indeed this is a consequence of the group axioms—see 1.1.2.

It is customary not to distinguish between the group $(G, \circ)$ and its underlying set G provided there is no possibility of confusion as to the intended group operation. However it should be borne in mind that there are usually many possible group operations on a given set.

The *order* of a group is defined to be the cardinality of the underlying set G. This is written $|G|$. If the group operation is *commutative*, that is, if $x \circ y = y \circ x$ is always valid, the group $(G, \circ)$ is called *abelian*.†

Before giving some standard examples of groups we shall list the most immediate consequences of the group axioms. The first of these is a generalization of the associative law to four or more elements.

1.1.1 (Generalized Associative Law). *If an element of a group is constructed from a sequence of elements $x_1, x_2, \dots, x_n$ in this order by repeatedly inserting brackets and applying the group operation, the element must equal*

$$(\cdots((x_1 \circ x_2) \circ x_3)\cdots) \circ x_n$$

and so is independent of the mode of bracketing.

Proof. Certainly we may assume that $n > 2$. If u is an element constructed from $x_1, x_2, \dots, x_n$ in the prescribed manner, we can write $u = v \circ w$ where v and w are constructed from $x_1, x_2, \dots, x_i$ and $x_{i+1}, \dots, x_n$ respectively $(1 \leq i < n)$. If $w = x_n$, the result follows by induction on n. Otherwise we can write $w = w' \circ x_n$ and $u = (v \circ w') \circ x_n$: once again the result follows by induction on n. □

Consequently in any expression formed from the elements $x_1, \dots, x_n$ in that order brackets can be omitted without ambiguity, an enormous simplification in notation.

1.1.2. *Let x be an element of a group G, let e be a right identity and let y be a right inverse of x. Then:*

(i) $y \circ x = e$;
(ii) $e \circ x = x$; *and*
(iii) *e is the unique left identity and the unique right identity; y is the unique left inverse of x and the unique right inverse of x.*

Proof. (i) Let $z = y \circ x$; then $z \circ z = y \circ (x \circ y) \circ x = z$ by 1.1.1. Now there is a w in G such that $z \circ w = e$. Since $z \circ z = z$, we have $z \circ (z \circ w) = z \circ w$ or $z = e$.

(ii) By (i) we have $x = x \circ e = x \circ (y \circ x) = (x \circ y) \circ x = e \circ x$.

(iii) By (ii) a right identity is a left identity. If e' is any left identity, then $e' = e' \circ e = e$. By (i) a right inverse of x is a left inverse. If t is any left inverse of x, then $t = t \circ (x \circ y) = (t \circ x) \circ y = y$. □

† After Niels Henrik Abel (1802–1829).

In view of the last result it is meaningful to speak of *the* identity of G and *the* inverse of x in G.

There are two commonly used ways of writing the group operation of a group $(G, \circ)$. In the *additive notation* $x \circ y$ is written as a "sum" $x + y$ and the identity element 0_G or 0, while $-x$ denotes the inverse of x. This notation is often used for abelian groups. We shall generally employ the *multiplicative notation* wherein $x \circ y$ is written as a "product" xy, the identity element is 1_G or 1 and x^{-1} is the inverse of x.

1.1.3. *In any (multiplicative) group the equation $xa = b$ implies that $x = ba^{-1}$ and the equation $ax = b$ implies that $x = a^{-1}b$.*

Proof. If $xa = b$, then $x = (xa)a^{-1} = ba^{-1}$: similarly for the second part. □

1.1.4. *In any group $(xy)^{-1} = y^{-1}x^{-1}$ and $(x^{-1})^{-1} = x$.*

Proof. Let $z = (xy)^{-1}$; then $xyz = 1$, whence $yz = x^{-1}$ and $z = y^{-1}x^{-1}$ by 1.1.3. Since $xx^{-1} = 1$, we have $x = (x^{-1})^{-1}$ by 1.1.3 again. □

Powers of an Element

Let x be an element of a multiplicatively written group G and let n be an integer. The nth *power* x^n of x is defined recursively in the following manner:

(i) $x^0 = 1_G$, $x^1 = x$, and x^{-1} is the inverse of x;
(ii) $x^{n+1} = x^n x$ if $n > 0$; and
(iii) $x^n = (x^{-n})^{-1}$ if $n < 0$.

Naturally, if G is written additively, we shall write nx instead of x^n and speak of a *multiple* of x.

1.1.5 (The Laws of Exponents). *Let m and n be integers and let x be an element of a group G. Then:*

(i) $x^m x^n = x^{m+n} = x^n x^m$; *and*
(ii) $(x^m)^n = x^{mn} = (x^n)^m$.

Proof. (i) Let $m \geq 0$ and $n \geq 0$; then by induction on n and the definition $x^m x^n = x^{m+n}$. Applying 1.1.3 we deduce that $x^n = x^{-m}x^{m+n}$ and $x^m = x^{m+n}x^{-n}$. Finally inversion of the equation $x^m x^n = x^{m+n}$ and application of 1.1.4 yield $x^{-n}x^{-m} = x^{-m+(-n)}$. Hence the law is established in all cases.

(ii) If $n \geq 0$, it follows from (i) that $(x^m)^n = x^{mn}$. Now assume that $n < 0$; then $(x^m)^n = ((x^m)^{-n})^{-1} = (x^{-mn})^{-1} = x^{mn}$ since $x^{-mn}x^{mn} = 1$. □

Isomorphism

If G and H are groups, a function $\alpha: G \to H$ is called an *isomorphism* if it is a *bijection* (or one–one correspondence) and if $(xy)\alpha = (x)\alpha \cdot (y)\alpha$. The symbolism $G \simeq H$ signifies that there is at least one isomorphism from G to H. If $\alpha: G \to H$ is an isomorphism, an application of α to $1_G 1_G = 1_G$ shows that $1_G\alpha = 1_H$, and to $xx^{-1} = 1_G$ that $(x^{-1})\alpha = (x\alpha)^{-1}$. It is easy to prove that isomorphism is an equivalence relation on groups.

One can see from the definition that isomorphic groups have exactly corresponding underlying sets and group operations. Thus any property of a group deducible from its cardinality and group operation will be possessed by all groups isomorphic to it. For this reason one is not usually interested in distinguishing between a group and groups that are isomorphic to it.

Exercises 1.1

1. Show that a semigroup with a left identity and left inverses is a group.
2. The identity $(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1} x_1^{-1}$ holds in any group.
3. If the identity $x^2 = 1$ holds in a group G, then G is abelian.
4. Show from first principles that a group of even order contains an *involution*, that is, an element $g \neq 1$ such that $g^2 = 1$.
5. The equation $(xy)^n = x^n y^n$ holds identically in a group for all n if and only if the group is abelian.

1.2. Examples of Groups

We shall now review some of the more obvious sources of groups.

(i) Groups of Numbers

Let $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote respectively the sets of all integers, rational numbers, real numbers, and complex numbers. Each set becomes a group if we specify ordinary addition as the group operation, zero as the identity and minus x as the inverse of x. The axioms of arithmetic guarantee the validity of the group axioms as well as the commutativity of the group operation. Thus all four groups are abelian.

The sets $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$, and $\mathbb{C}\backslash\{0\}$ are groups with respect to multiplication, 1 being the identity and $1/x$ being the inverse of x. Again all the groups are abelian.

(ii) Groups of Matrices

Let R be a ring with an identity element and let $\mathrm{GL}(n, R)$ denote the set of all $n \times n$ matrices with coefficients in R which have inverses (these are to be $n \times n$ matrices over the ring R). Taking matrix multiplication as the group operation, we see from elementary properties of matrices that $\mathrm{GL}(n, R)$ is a group whose identity element is 1_n, the $n \times n$ identity matrix. This group is called the *general linear group* of degree n over R. It is nonabelian if $n > 1$. In particular, if F is a field, $\mathrm{GL}(n, F)$ is the group of all nonsingular $n \times n$ matrices over F.

(iii) Groups of Linear Transformations

If V is an n-dimensional vector space over a field F, let $\mathrm{GL}(V)$ denote the set of all bijective linear transformations of V. Then $\mathrm{GL}(V)$ is a group if functional composition is specified as the group operation: thus $(v)\alpha \circ \beta = ((v)\alpha)\beta$ where $v \in V$ and $\alpha, \beta \in \mathrm{GL}(V)$.

There is a close connection between the groups $\mathrm{GL}(V)$ and $\mathrm{GL}(n, F)$. For, if a fixed ordered basis for V is chosen, each bijective linear transformation of V is associated with a nonsingular $n \times n$ matrix over F. This correspondence is an isomorphism from $\mathrm{GL}(V)$ to $\mathrm{GL}(n, F)$, the reason being that when two linear transformations are composed, the product of the corresponding matrices represents the composite. These facts can be found in most text books on linear algebra.

(iv) Groups of Isometries

Let M be a metric space with a distance function $d: M \times M \to \mathbb{R}$. An *isometry* of M is a bijective mapping $\alpha: M \to M$ which preserves distances; thus

$$(x\alpha, y\alpha)d = (x, y)d$$

for all x, y in M. It is very easy to verify that the set of all isometries of M is a group with respect to the operation of functional composition. We shall write this group

$$\mathrm{Isom}(M).$$

Suppose next that X is a nonempty subset of M. If α is an isometry, define $X\alpha$ to be the set $\{x\alpha \mid x \in X\}$. The *symmetry group* of X with respect to the metric space M is the set

$$S_M(X) = \{\alpha \in \mathrm{Isom}(M) \mid X\alpha = X\}$$

of all isometries that leave X fixed as a set, together with functional composition. Again it is clear that this is a group. The more "symmetrical" the set

X, the larger is the symmetry group. Thus we arrive at the fundamental idea of a group as a measure of the symmetry of a structure. It is one reason for the prevalence of groups in so many areas of science.

(v) Isometries of E^2

Let E^n denote n-dimensional Euclidean space. We shall give a brief account of isometries and symmetries in E^2. For a detailed study of isometries in E^2 and in E^3 see [b11].

There are three natural types of isometry in E^2, *rotations* about a point, *reflections* in a line, and *translations*: in the latter the point (x, y) is moved to $(x + a, y + b)$ for some fixed a, b. It can be shown that every isometry is a rotation, a translation, a reflection, or the product of a reflection and a translation.

If X is a bounded subset of E^2, it is intuitively clear that an isometry leaving X invariant cannot be a translation, and in fact must be a rotation or a reflection.

Let us use the preceding remarks to analyze a famous example. Let X be a regular polygon with n edges ($n \geq 3$). The rotations that leave X invariant are about the center of X through angles $2\pi i/n$, $i = 0, 1, \dots, n - 1$. The reflections which preserve X are in lines joining opposite vertices or midpoints of opposite edges if n is even, or in lines through a vertex and the midpoint of the opposite edge if n is odd. Thus in all $S_{E^2}(X)$ contains $n + n = 2n$ elements. This group is called the *dihedral group* of order $2n$; it is written

$$D_{2n}.$$

(The reader is warned that some authors denote this group by D_n.)

(vi) Groups of Permutations

If X is a nonempty set, a bijection $\pi\colon X \to X$ is called a *permutation* of X. The set of all permutations of X is a group with respect to functional composition called the *symmetric* group on X,

$$\text{Sym } X.$$

When $X = \{1, 2, \dots, n\}$, it is customary to write

$$S_n$$

for Sym X, and to call this the *symmetric group of degree n*.

Historically the first groups to be studied systematically were groups of permutations (or substitutions, as they were called). This approach is not so limited as it might seem since by a fundamental result (1.6.8) every group is isomorphic with a group of permutations of its underlying set.

We remind the reader that the *signature* of a permutation $\pi \in S_n$ is defined to be

$$\operatorname{sign} \pi = \prod_{1 \leq i < j \leq n} \frac{(i)\pi - (j)\pi}{i - j},$$

which equals $+1$ or -1. Recall that π is *even* if sign $\pi = +1$ and *odd* if sign $\pi = -1$. From the definition it is easy to check the formulas

$$\operatorname{sign}(\pi_1 \pi_2) = (\operatorname{sign} \pi_1)(\operatorname{sign} \pi_2) \qquad \text{and} \qquad \operatorname{sign}(\pi^{-1}) = \operatorname{sign} \pi.$$

Hence the set of all even permutations in S_n is also a group with respect to functional composition; this is the *alternating group* A_n. Obviously $|A_1| = 1$; if $n > 1$, the function $\pi \mapsto \pi(1, 2)$ is a bijection from A_n to the set of all odd permutations in S_n; hence $|A_n| = \frac{1}{2}(n!)$.

Exercises 1.2

1. Prove that no two of the groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are isomorphic.
2. Let R be a ring with identity. Prove that $\mathrm{GL}(n, R)$ is abelian if and only if $n = 1$ and R^* is commutative. (Here R^* is the group of units, i.e., invertible elements of R.)
3. Describe the symmetry group of: (a) an isosceles but nonequilateral triangle; (b) a swastika.
4. Show that the symmetry group of a rectangle which is not a square has order 4. By labeling the vertices 1, 2, 3, 4, represent the symmetry group as a group of permutations of the set $\{1, 2, 3, 4\}$. (This is called a *Klein* 4-*group*.)
5. Represent the dihedral group D_{2n} as a group of permutations of the set $\{1, 2, \dots, n\}$ by labeling the vertices of a regular polygon with n edges.
6. Describe the symmetry group of $\mathbb{Z}$ in E^1. (This group, D_∞, is known as the *infinite dihedral group*.)
7. Exhibit all rotations of E^3 that leave invariant a regular tetrahedron. This group is called the *tetrahedral group*. Prove that it is isomorphic with A_4.
8. Show that the group of all rotations in E^3 that leave a cube invariant is isomorphic with S_4. [*Hint*: A rotation permutes the four diagonals of the cube.]
9. A regular *octahedron* is the polyhedron obtained by joining the centres of the faces of a cube. Prove that the rotation group of the octahedron is isomorphic with S_4 (sometimes known as the *octahedral group*).
10. Prove that Sym X is abelian if and only if $|X| \leq 2$.
11. Give a group-theoretic proof of Wilson's Theorem: if p is a prime, then $(p-1)! \equiv -1 \pmod{p}$. [*Hint*: Form the product of all the elements of the group $\mathbb{Z}_p^*$.]

1.3. Subgroups and Cosets

Let G be a group and let H be a subset of G. We say that H is a *subgroup* of G if $(H, *)$ is a group where $*$ is the group operation of G restricted to H. From 1.1.3 and the equation $1_H 1_H = 1_H$ it follows that $1_H = 1_G$. Also, if x_H^{-1} is the inverse of x *in the group* $(H, *)$, then $xx_H^{-1} = 1_H = 1_G$, whence $x_H^{-1} = x^{-1}$. Thus identity and inverses are the same in G and in H. From this it is clear that a subset H is a subgroup of G if and only if it contains the identity and all products and inverses of its elements.

We shall write

$$H \leq G \qquad \text{or} \qquad G \geq H$$

to signify that H is a subgroup of G. Two obvious examples of subgroups are the *trivial* or *identity subgroup* $\{1_G\}$, usually written 1_G or 1, and the *improper subgroup* G itself. If $H \leq G$ and $H \neq G$, then G is called a *proper subgroup* of G; in symbols $H < G$ or $G > H$.

1.3.1 (The Subgroup Criterion). *Let H be a subset of a group G. Then H is a subgroup of G if and only if H is not empty and $xy^{-1} \in H$ whenever $x \in H$ and $y \in H$.*

Proof. Necessity being clear, assume that the conditions hold: then there exists an $h \in H$ and $1_G = hh^{-1} \in H$. If $x, y \in H$, then $1_G y^{-1} = y^{-1} \in H$ and hence $x(y^{-1})^{-1} = xy \in H$. Thus H is a subgroup. □

Examples of Subgroups

(i) $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are subgroups of $\mathbb{C}$.

(ii) Let R be a commutative ring with identity. Define $\mathrm{SL}(n, R)$ to be the set of all $n \times n$ matrices over R with determinant equal to 1. Since $\det(AB^{-1}) = (\det A)(\det B)^{-1}$ and $\mathrm{SL}(n, R)$ contains the identity matrix, we see from 1.3.1 that $\mathrm{SL}(n, R)$ is a subgroup of $\mathrm{GL}(n, R)$; it is called the *special linear group of degree n over R*.

(iii) A_n is a subgroup of S_n. This follows from 1.3.1 and the equation $\mathrm{sign}(\pi_1 \pi_2^{-1}) = (\mathrm{sign}\ \pi_1)(\mathrm{sign}\ \pi_2)$.

Intersections and Joins of Subgroups

1.3.2. *If $\{H_\lambda | \lambda \in \Lambda\}$ is a set of subgroups of a group G, then $I = \bigcap_{\lambda \in \Lambda} H_\lambda$ is a subgroup of G.*

Proof. Obviously $1 \in I$. If $x, y \in I$, then $x, y \in H_\lambda$ and hence $xy^{-1} \in H_\lambda$ for all $\lambda \in \Lambda$. Thus $xy^{-1} \in I$ and $I \leq G$ by 1.3.1. □

The Subgroup Generated by a Subset

Let X be a nonempty subset of a group G. Define *the subgroup generated by* X

$$\langle X \rangle$$

to be the intersection of all subgroups of G which contain X: notice that there will always be at least one such subgroup, G itself. That $\langle X \rangle$ *is* a subgroup follows from 1.3.2. In a real sense $\langle X \rangle$ is the *smallest* subgroup of G containing X: for if $X \subseteq S \leq G$, then $\langle X \rangle \subseteq S$. Clearly $X = \langle X \rangle$ precisely when X itself is a subgroup.

Naturally one wishes to have a description of the elements of $\langle X \rangle$.

1.3.3. *If X is a nonempty subset of a group G, then $\langle X \rangle$ is the set of all elements of the form $x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k}$ where $\varepsilon_i = \pm 1$, $x_i \in X$, and $k \geq 0$. (When $k = 0$, the product is to be interpreted as* 1.)

Proof. Let S denote the set of all such elements. Then S is a subgroup by 1.3.1, while clearly $X \subseteq S$: hence $\langle X \rangle \subseteq S$. But obviously $S \subseteq \langle X \rangle$, so that $S = \langle X \rangle$. □

If n is a positive integer, a group is said to be an *n-generator group* if it can be generated by some n-subset $\{x_1, x_2, \ldots, x_n\}$. A group is *finitely generated* if it is n-generator for some n.

A 1-generator group $\langle x \rangle \equiv \langle \{x\} \rangle$ is termed *cyclic*: by 1.3.3 this consists of all the powers of x. The standard example of an infinite cyclic group is $\mathbb{Z}$, while $\mathbb{Z}_n$, the additive group of congruence classes modulo n, is the standard cyclic group of order n.

If $\{X_\lambda | \lambda \in \Lambda\}$ is a set of subgroups of G, the *join of the X_λ's* or the *subgroup generated by the X_λ's* is defined to be $\langle \bigcup_{\lambda \in \Lambda} X_\lambda \rangle$. This will be written

$$\langle X_\lambda | \lambda \in \Lambda \rangle$$

or in case $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$, a finite set,

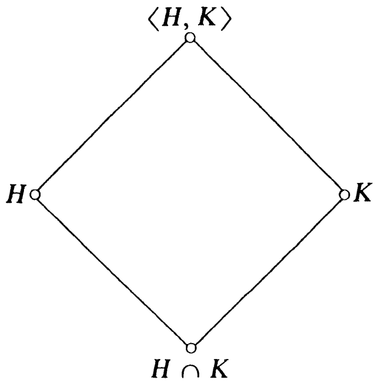
$$\langle X_{\lambda_1}, \ldots, X_{\lambda_n} \rangle.$$

If G is any group, the set $\mathbf{S}(G)$ of all subgroups of G is a partially ordered set with respect to set inclusion. Moreover a nonempty subset of $\mathbf{S}(G)$ has a least upper bound in $\mathbf{S}(G)$, the join of all its elements, and a greatest lower bound in $\mathbf{S}(G)$, the intersection of all its elements. Thus $\mathbf{S}(G)$ *is a complete lattice*, known as *the subgroup lattice of* G. The unique smallest element of $\mathbf{S}(G)$ is 1, the unique largest G.

Hasse Diagrams

It is sometimes helpful to visualize the inclusions which exist between subgroups of a group by means of a *Hasse diagram*. In this subgroups are

represented by vertices, while an ascending edge or sequence of ascending edges joining two subgroups indicates that the lower subgroup is contained in the upper subgroup. The basic Hasse diagram is the so-called *parallelogram diagram.*



Left and Right Cosets

If H is a fixed subgroup of a group G, a relation $\sim_H$ on G is defined in the following way: $x \sim_H y$ holds if and only if $x = yh$ for some $h \in H$. It is easy to check that $\sim_H$ is an equivalence relation on G and that the equivalence class containing x is the subset xH defined by

$$xH = \{xh | h \in H\}:$$

this is called the *left coset* of H containing x. Observe that distinct left cosets are disjoint and $xH = yH$ if and only if $x^{-1}y \in H$. All left cosets of H have the cardinality of H in view of the bijection $h \mapsto xh$ from H to xH. The union of all the left cosets of H is G.

Let us select an element from each left coset of H (thereby using the axiom of choice!) and write T for the resulting set of *left coset representatives.* Then G is the disjoint union

$$G = \bigcup_{t \in T} tH$$

and every element of G can be uniquely written in the form th, $t \in T$, $h \in H$. The set T is called a *left transversal* to H in G. Notice that $|T|$ equals the cardinality of the set of left cosets of H. Frequently it is convenient to choose 1 as the coset representative of H, so that $1 \in T$.

In a precisely similar way the *right coset*

$$Hx = \{hx | h \in H\}$$

arises as the ${}_H\sim$-equivalence class containing x where $x \,{}_H\sim\, y$ means that $x = hy$ for some $h \in H$. The terms *right coset representative* and *right transversal* are defined analogously.

Products and Inverses of Subsets

It is useful to generalize the notion of a coset. If X and Y are arbitrary nonempty subsets of a group, define their *product* to be the subset

$$XY = \{xy | x \in X, y \in Y\}$$

and the *inverse* of X to be

$$X^{-1} = \{x^{-1} | x \in X\}.$$

Then clearly $xH = \{x\}H$ is a left coset and $Hx = H\{x\}$ a right coset if $H \leq G$. Multiplication of subsets is associative and $(X^{-1})^{-1} = X$ is always valid.

More generally we define the product of a family of subsets

$$X_1 X_2 \cdots X_k;$$

this consists of all products $x_1 x_2 \cdots x_k$ where $x_i \in X_i$. Of course we speak of a *sum* of subsets in the case of an additive group.

1.3.4. *Let H be a subgroup of G and let T be a left transversal to H in G. Then T^{-1} is a right transversal to H in G. In particular, the sets of left and right cosets of H have the same cardinality.*

Proof. Since G is the disjoint union of the tH, $t \in T$, inversion shows that $G^{-1} = G$ is the disjoint union of the $(tH)^{-1} = Ht^{-1}$. □

The cardinality of the set of left (or right) cosets of H in G is called the *index* of H in G and is written

$$|G:H|.$$

1.3.5. *Let $K \leq H \leq G$. If T is a left transversal to H in G and U a left transversal to K in H, then TU is a left transversal to K in G. Thus*

$$|G:K| = |G:H| \cdot |H:K|.$$

Proof. $G = \bigcup_{t \in T} tH$ and $H = \bigcup_{u \in U} uK$, whence $G = \bigcup_{t \in T, u \in U} tuK$. It remains to show that all the cosets tuK are distinct. Suppose that $tuK = t'u'K$ where $t, t' \in T$ and $u, u' \in U$: then $t^{-1}t' \in H$ and $tH = t'H$. Since T is a transversal, $t = t'$; hence $uK = u'K$ and $u = u'$ since U is a transversal. □

Specializing to the case $K = 1$, we obtain a fundamental theorem.

1.3.6 (Lagrange's Theorem). *If G is a group and H is a subgroup of G, then $|G| = |G:H| \cdot |H|$. If G is finite, $|G:H| = |G|/|H|$. Hence the order of a subgroup always divides the order of the group if the latter is finite.*

On the other hand, just because a positive integer divides the group order it does not follow that there is a subgroup with this order (see Exercise 1.3.3).

Double Cosets

If H and K are subgroups and x is an element of a group G, the subset

$$HxK = \{hxk \mid h \in H, k \in K\}$$

is called an *(H, K)-double coset*. There is a partition of the group into double cosets which is occasionally useful.

1.3.7. *Let H and K be subgroups of a group G.*

(i) *The group G is a union of (H, K)-double cosets.*
(ii) *Two (H, K)-double cosets are either equal or disjoint.*
(iii) *The double coset HxK is a union of right cosets of H and a union of left cosets of K.*

Proof. Define $x \sim y$ to mean that $x = hyk$ for some h in H and k in K. It is easy to check that $\sim$ is an equivalence relation on G, the equivalence class containing x being HxK. Thus (i) and (ii) follow at once. (iii) is clear. □

The Order of an Element

A group element x has *finite order n* if the cyclic subgroup $\langle x \rangle$ has order n. If $\langle x \rangle$ is infinite, then x has *infinite order*. We shall write

$$|x|$$

for the order of x. Elements of order 2 are often called *involutions*.

A *torsion group* (or *periodic group*) is a group all of whose elements have finite order. If the orders of the elements of a group are finite and bounded, the group is said to have *finite exponent*. The *exponent* of the group is then the least common multiple of all the orders. Obviously a finite group has finite exponent and a group with finite exponent is a torsion group.

On the other hand, a group is said to be *torsion-free* (or *aperiodic*) if apart from the identity all its elements have infinite order.

1.3.8. *Let x be an element of a group G.*

(i) *x has infinite order if and only if all powers of x are distinct.*
(ii) *If x has finite order n, then $x^m = 1$ if and only if $n \mid m$. Moreover $\langle x \rangle$ consists of the distinct elements $1, x, x^2, \ldots, x^{n-1}$.*
(iii) *If x has finite order n, the order of x^k equals $n/(n, k)$.*

Proof. If all powers of x are distinct, $\langle x \rangle$ is obviously infinite. Conversely suppose that two powers of x are equal, say $x^l = x^m$ where $l < m$; then $x^{m-l} = 1$. Thus we can choose the least positive integer n such that $x^n = 1$. Using the division algorithm we may write an arbitrary integer m in the form $m = qn + r$ where q, r are integers and $0 \leq r < n$. Then $x^m = (x^n)^q x^r = x^r$, which shows that $\langle x \rangle = \{1, x, \dots, x^{n-1}\}$. Hence x has finite order. Also $x^m = 1$ if and only if $r = 0$, that is, if $n|m$: this is by minimality of n. Next suppose that $x^i = x^j$ where $0 \leq i \leq j < n$. Then $x^{j-i} = 1$, so that $n | j - i$: but this can only mean that $i = j$. Hence the elements $1, x, \dots, x^{n-1}$ are all distinct and $|x| = n$. Thus (i) and (ii) are established.

To prove (iii) observe that $(x^k)^{n/(n,k)} = (x^n)^{k/(n,k)} = 1$, which implies that $m = |x^k|$ divides $n/(n, k)$. Also since $(x^k)^m = 1$, one has that $n|km$ and hence that $n/(n, k)$ divides $(k/(n, k))m$. By Euclid's Lemma $n/(n, k)$ divides m, so $m = n/(n, k)$. □

Subgroups of Cyclic Groups

While it can be an arduous task to determine all the subgroups of a group, there is little difficulty in the case of cyclic groups.

1.3.9. *Let $G = \langle x \rangle$ and let H be a subgroup of G.*

(i) *If G is infinite, then H is either infinite cyclic or trivial.*
(ii) *If G has finite order n, then H is cyclic of order dividing n. Conversely, to each positive divisor d of n there corresponds exactly one subgroup of order d, namely $\langle x^{n/d} \rangle$.*

Proof. We prove first that H is cyclic. If $H = 1$, this is obvious, so let $H \neq 1$; then H contains some positive power $x^s \neq 1$. Let s be chosen minimal with this property. Clearly $\langle x^s \rangle \subseteq H$. If $x^t \in H$, write $t = sq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < s$. Then $x^r = (x^s)^{-q} x^t \in H$, so the minimality of s shows that $r = 0$ and $s|t$. Hence $x^t \in \langle x^s \rangle$ and $H = \langle x^s \rangle$. If G is infinite, x has infinite order, as does x^s. Hence H is an infinite cyclic group.

Now let $|x| = n < \infty$. Then $|H|$ divides n, as we see at once from Lagrange's Theorem. Conversely suppose that $d|n$; then $|x^{n/d}| = d$ by 1.3.8 and $|\langle x^{n/d} \rangle| = d$. Finally suppose that $\langle x^k \rangle$ is another subgroup of order d. Then $x^{kd} = 1$ and $n|kd$: consequently n/d divides k and $\langle x^k \rangle \leq \langle x^{n/d} \rangle$. But these subgroups both have order d, so they coincide. □

It is obvious that a group has just one subgroup if and only if it has order 1. We determine next the groups with exactly two subgroups.

1.3.10. *A group G has precisely two subgroups, namely* 1 *and G, if and only if it is cyclic of prime order.*

Proof. Sufficiency is immediate from 1.3.6. If G has only two subgroups and $1 \neq x \in G$, then $G = \langle x \rangle$. Moreover, should $|x|$ be infinite, $\langle x^2 \rangle$ will be a proper nontrivial subgroup. Hence $|x|$ is finite and by 1.3.9 it must be prime. □

Index Theorems

We shall record some basic properties of the index of a subgroup.

1.3.11. *Let H and K be subgroups of a group G.*

(i) $|HK| \cdot |H \cap K| = |H| \cdot |K|$, *so that* $|H : H \cap K| = |HK|/|K|$ *if H and K are finite.*
(ii) $|G : H \cap K| \leq |G : H| \cdot |G : K|$, *with equality if the indices* $|G : H|$ *and* $|G : K|$ *are finite and coprime.*

Proof. (i) Define an equivalence relation $\sim$ on the set product $H \times K$ by the rule $(h, k) \sim (h', k')$ if and only if $hk = h'k'$; this is equivalent to $h^{-1}h' = k(k')^{-1}$ or to $(h', k') = (hi, i^{-1}k)$ for some $i \in H \cap K$. Hence the equivalence class $\overline{(h, k)}$ containing (h, k) has cardinality $|H \cap K|$. Now consider the function $(h, k) \mapsto hk$: elements equivalent to (h, k) also map to hk, so we have a function from the set of equivalence classes to HK given by $\overline{(h, k)} \mapsto hk$. Moreover this function is bijective by definition of $\sim$. Hence the set of all equivalence classes has cardinality $|HK|$. Since $|H \times K| = |H| \cdot |K|$, it follows that $|H| \cdot |K| = |HK| \cdot |H \cap K|$.

(ii) To each left coset $x(H \cap K)$ we assign the pair of left cosets (xH, xK): this pair is clearly well-defined. Now $(xH, xK) = (x'H, x'K)$ if and only if $x^{-1}x' \in H \cap K$ or $x(H \cap K) = x'(H \cap K)$. Therefore the assignment $x(H \cap K) \mapsto (xH, xK)$ is an injection and

$$|G : H \cap K| \leq |G : H| \cdot |G : K|.$$

If $|G : H|$ and $|G : K|$ are finite and relatively prime, each divides $|G : H \cap K|$ by 1.3.5, whence their product does too. □

1.3.12 (Poincaré). *The intersection of a finite set of subgroups each of which has finite index is itself of finite index.*

The important result is an immediate consequence of 1.3.11(ii).

Permutable Subgroups and Normal Subgroups

Two subgroups H and K of a group G are said to *permute* if $HK = KH$. This is in fact precisely the condition for HK to be a subgroup.

1.3.13. *If H and K are subgroups of a group, then HK is a subgroup if and only if H and K permute. In this event $HK = \langle H, K\rangle = KH$.*

Proof. Suppose that $HK \leq G$; then $H \leq HK$ and $K \leq HK$, so $KH \subseteq HK$. Taking inverses of each side we get $HK \subseteq KH$, whence $HK = KH$. Moreover $\langle H, K\rangle \leq HK$ since $HK \leq G$, while $HK \subseteq \langle H, K\rangle$ is always true; thus $\langle H, K\rangle = HK$. Conversely let $HK = KH$: if $h_i \in H$ and $k_i \in K$, then

$$h_1k_1(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1}:$$

now $(k_1k_2^{-1})h_2^{-1} = h_3k_3$ where $h_3 \in H$ and $k_3 \in K$. Hence $h_1k_1(h_2k_2)^{-1} = (h_1h_3)k_3 \in HK$ and $HK \leq G$ by 1.3.1. □

1.3.14 (Dedekind's† Modular Law). *Let H, K, L be subgroups of a group and assume that $K \subseteq L$. Then $(HK) \cap L = (H \cap L)K$. In particular, if H and K permute, $\langle H, K\rangle \cap L = \langle H \cap L, K\rangle$.*

Proof. In the first place $(H \cap L)K \subseteq HK$ and $(H \cap L)K \subseteq LK = L$: hence $(H \cap L)K \subseteq (HK) \cap L$. Conversely let $x \in (HK) \cap L$ and write $x = hk$, $(h \in H, k \in K)$: then $h = xk^{-1} \in LK = L$, so that $h \in H \cap L$. Hence $x \in (H \cap L)K$. The second part follows via 1.3.13. □

The reader should note that since $K \cap L = K$, the modular law is really a form of the distributive law $(HK) \cap L = (H \cap L)(K \cap L)$: however the latter is false in general.

A subgroup of a group G which permutes with every subgroup of G is said to be *permutable* (or *quasinormal*). By far the most important examples of permutable subgroups are *normal subgroups*: these are subgroups possessing one of the three equivalent properties in the next result.

1.3.15. *If H is a subgroup of a group G, the following statements about H are equivalent:*

(i) *$xH = Hx$ for all $x \in G$;*
(ii) *$x^{-1}Hx = H$ for all $x \in G$; and*
(iii) *$x^{-1}hx \in H$ for all $x \in G$, $h \in H$.*

Proof.

(i) ⇒ (ii). Premultiply by x^{-1}.

(ii) ⇒ (iii). This is clear.

(iii) ⇒ (i). Let $h \in H$ and $x \in G$. Then $hx = x(x^{-1}hx) \in xH$ and $xh = (x^{-1})^{-1}hx^{-1} \cdot x \in Hx$. Hence $xH = Hx$. □

The notation

$$H \lhd G$$

† Richard Dedekind (1831–1916).

signifies that H is a normal subgroup of G. Of course 1 and G are normal subgroups and these may well be the only normal subgroups of G. If this is the case and $G \neq 1$, the group G is said to be *simple*. More interesting instances of normality are: $A_n \lhd S_n$ and $\mathrm{SL}(n, R) \lhd \mathrm{GL}(n, R)$. Note also that in an abelian group every subgroup is normal.

It follows from 1.3.15 that a *normal subgroup is permutable*: hence the product of a subgroup and a normal subgroup is always a subgroup.

1.3.16. *If $\{N_\lambda | \lambda \in \Lambda\}$ is a collection of normal subgroups of a group, then $\bigcap_{\lambda \in \Lambda} N_\lambda$ and $\langle N_\lambda | \lambda \in \Lambda \rangle$ are normal subgroups.*

Proof. The first part is clear: to prove the second apply 1.3.3. □

Normal Closure and Core

If X is a nonempty subset of a group G, the *normal closure* of X in G is the intersection of all the normal subgroups of G which contain X. By 1.3.16 this is a normal subgroup; it is denoted by

$$X^G.$$

Clearly X^G is the smallest normal subgroup containing X and it is easy to show that $X^G = \langle g^{-1}Xg | g \in G \rangle$, cf. the proof of 1.3.3.

Dual to the normal closure is X_G the *normal interior* or *core* of X in G; this is defined to be the join of all the normal subgroups of G that are contained in X, with the convention that $X_G = 1$ if there are no such subgroups. Again it is simple to prove that $H_G = \bigcap_{g \in G} g^{-1}Hg$ for H a subgroup.

Exercises 1.3

1. If $H \leq G$, then $G \backslash H$ is finite if and only if G is finite or $H = G$.
2. Find all subgroups of S_3. Using a Hasse diagram display the subgroup lattice.
3. Repeat Exercise 2 for A_4, observing that A_4 has no subgroup of order 6.

*4. Let $d(G)$ be the smallest number of elements necessary to generate a finite group G. Prove that $|G| \geq 2^{d(G)}$. [*Note*: By convention $d(G) = 0$ if $|G| = 1$.]

5. A cyclic group of finite order n is isomorphic with $\mathbb{Z}_n$: an infinite cyclic group is isomorphic with $\mathbb{Z}$.

*6. If G is infinite cyclic and $1 \neq H \leq G$, then $|G : H|$ is finite.

7. A group has exactly three subgroups if and only if it is cyclic of order p^2 for some prime p.

*8. Let H and K be subgroups with coprime indices in a finite group G. Prove that $G = HK$ (use 1.3.11).

9. Let $H \leq G$ and $K \leq G$. Then $H \cup K \leq G$ if and only if $H \leq K$ or $K \leq H$. Deduce that no group is a union of two proper subgroups.

10. Give examples of: (a) a torsion group with infinite exponent; and (b) an infinite group with finite exponent.

11. Prove that $\mathbb{Q}$ is not finitely generated.

12. Let H and K be subgroups of a finite group G.

    (a) Show that the number of right cosets of H in HdK equals $|K : H^d \cap K|$.
    (b) Prove that
    $$\sum_d \frac{1}{|H^d \cap K|} = \frac{|G|}{|H| \cdot |K|} = \sum_d \frac{1}{|H \cap K^d|}$$
    where d runs over a set of (H, K)-double coset representatives.

13. A subgroup of index 2 is always normal.

14. Given that $H_\lambda \lhd K_\lambda \leq G$ for all λ in Λ, show that $\bigcap_\lambda H_\lambda \lhd \bigcap_\lambda K_\lambda$.

*15. Show that normality is not a transitive relation (check D_8).

*16. If $H \leq K \leq G$ and $N \lhd G$, show that the equations $HN = KN$ and $H \cap N = K \cap N$ imply that $H = K$.

*17. If $G = D_{2n}$, find elements x and y of orders 2 and n respectively such that $G = \langle x, y \rangle$ and $x^{-1}yx = y^{-1}$.

*18. If $H \leq G$, prove that $H^G = \langle H^g | g \in G \rangle$ and $H_G = \bigcap_{g \in G} H^g$.

19. Show that $(HK) \cap L = (H \cap L)(K \cap L)$ is not valid for all subgroups H, K, L.

1.4. Homomorphisms and Quotient Groups

Let G and H be two groups. A function $\alpha: G \to H$ is called a *homomorphism* if
$$(xy)\alpha = (x\alpha)(y\alpha)$$
for all $x, y \in G$. For multiplicative groups it is advantageous to write x^α instead of $x\alpha$, so that the above becomes
$$(xy)^\alpha = x^\alpha y^\alpha.$$
The set of all homomorphisms from G to H is denoted by
$$\mathrm{Hom}(G, H).$$
This set is always nonempty since it contains the *zero homomorphism* $0: G \to H$ which sends every element of G to 1_H.

A homomorphism $\alpha: G \to G$ is called an *endomorphism* of G. The identity function $1: G \to G$ is clearly an endomorphism.

Of the greatest importance are the *image* Im α and the *kernel* Ker α of a homomorphism $\alpha: G \to H$. These subsets are defined as follows:

$$\text{Im}\,\alpha \equiv G^\alpha = \{x^\alpha | x \in G\}$$

and

$$\text{Ker}\,\alpha = \{x | x \in G, x^\alpha = 1_H\}.$$

1.4.1. *Let $\alpha: G \to H$ be a homomorphism.*

(i) $(x^n)^\alpha = (x^\alpha)^n$ *for all integers n, so that* $1_G^\alpha = 1_H$.
(ii) Im $\alpha \leq H$ *and* Ker $\alpha \lhd G$.

Proof. (i) For $n > 0$ this is easily proved by induction on n, while the case $n = 0$ is dealt with as follows: $1_G^\alpha = (1_G 1_G)^\alpha = 1_G^\alpha 1_G^\alpha$, whence $1_G^\alpha = 1_H$ by 1.1.3. Let $n < 0$: then $x^n x^{-n} = 1_G$, so $(x^n)^\alpha (x^{-n})^\alpha = 1_H$ and $(x^n)^\alpha = ((x^{-n})^\alpha)^{-1} = ((x^\alpha)^{-n})^{-1} = (x^\alpha)^n$.

(ii) This follows from the subgroup criterion and the definition of normality. □

The group $G/\text{Ker}\,\alpha$ is sometimes called the *coimage of* α: if Im $\alpha \lhd H$, then $H/\text{Im}\,\alpha$ is the *cokernel of* α.

Examples of Homomorphisms

(i) $\alpha: S_n \to \langle -1 \rangle$ where $\pi^\alpha = \text{sign}\,\pi$.
(ii) $\alpha: \text{GL}(n, F) \to F^*$ where $A^\alpha = \det A$ and $F^* = F \backslash \{0\}$. Here F is a field.

Monomorphisms, Epimorphisms, and Isomorphisms

An injective (or one–one) homomorphism is called a *monomorphism* and a surjective (or onto) homomorphism an *epimorphism*: of course a bijective homomorphism is what we have been calling an *isomorphism*.

1.4.2. *Let $\alpha: G \to H$ be a homomorphism.*

(i) α *is a monomorphism if and only if* Ker $\alpha = 1_G$.
(ii) α *is an epimorphism if and only if* Im $\alpha = H$.
(iii) α *is an isomorphism if and only if* Ker $\alpha = 1_G$ *and* Im $\alpha = H$.

Proof. If α is a monomorphism and $x \in \text{Ker}\,\alpha$, then $x^\alpha = 1_H = 1_G^\alpha$, whence $x = 1_G$ by injectivity. Conversely let Ker $\alpha = 1_G$; then $x^\alpha = y^\alpha$ implies that $(xy^{-1})^\alpha = 1_H$, so $xy^{-1} \in \text{Ker}\,\alpha = 1_G$ and $x = y$. The rest is clear. □

Quotient Groups and the Noether† Isomorphism Theorems

If N is a normal subgroup of a group G, the *quotient group* (or *factor group*) of N in G,

$$G/N,$$

is the set of all cosets of N in G equipped with the group operation

$$(Nx)(Ny) = N(xy).$$

This operation is well-defined since if $x' = ax$ and $y' = by$ with $a, b \in N$, then $x'y' = axby = a(xbx^{-1})xy \in Nxy$. Associativity is immediate. The inverse of Nx is Nx^{-1} and the identity element is N. Clearly $|G/N| = |G : N|$. It is often convenient to use the congruence notation

$$x \equiv y \mod N$$

in place of $Nx = Ny$.

The next theorem shows the very intimate relation between quotient groups and homomorphisms.

1.4.3 (First Isomorphism Theorem)

(i) *If* $\alpha: G \to H$ *is a homomorphism of groups, the mapping* θ: $(\text{Ker } \alpha)x \mapsto x^\alpha$ *is an isomorphism from* $G/\text{Ker } \alpha$ *to* $\text{Im } \alpha$.
(ii) *If* N *is a normal subgroup of a group* G, *the mapping* $v: x \mapsto Nx$ *is an epimorphism from* G *to* G/N *with kernel* N. (*This* v *is called the natural or canonical homomorphism.*)

Proof. (i) Recall from 1.4.1 that $\text{Ker } \alpha \lhd G$. Now θ is well-defined since $(kx)^\alpha = x^\alpha$ if $k \in \text{Ker } \alpha$, and it is clearly an epimorphism. Also $(\text{Ker } \alpha)x \in \text{Ker } \theta$ if and only if $x \in \text{Ker } \alpha$, that is to say, $\text{Ker } \theta = 1_{G/\text{Ker } \alpha}$; thus θ is an isomorphism (by 1.4.2).

(ii) v is a homomorphism since $Nxy = (Nx)(Ny)$: it is obviously an epimorphism. Finally $x^v = 1_{G/N}$ if and only if $x \in N$. □

1.4.4 (Second Isomorphism Theorem). *Let* H *be a subgroup and* N *a normal subgroup of a group* G. *Then* $N \cap H \lhd H$ *and* $(N \cap H)x \mapsto Nx$ *is an isomorphism from* $H/N \cap H$ *to* NH/N.

Proof. The function $x \mapsto Nx$ is clearly an epimorphism from H to NH/N whose kernel is $N \cap H$. The result follows by 1.4.3(i). □

1.4.5 (Third Isomorphism Theorem). *Let* M *and* N *be normal subgroups of a group* G *and let* $N \leq M$. *Then* $M/N \lhd G/N$ *and*

$$(G/N)/(M/N) \simeq G/M.$$

† Emmy Noether (1882–1935).

Proof. Define α: $G/N \to G/M$ by $(Nx)^\alpha = Mx$. This is a well-defined epimorphism with kernel M/N. The result follows by 1.4.3(i). □

Subgroups of the Image

Suppose that $\alpha: G \to H$ is a homomorphism. If $S \leq G$, define S^α to be $\{s^\alpha | s \in S\}$, the image of the restriction $\alpha|_S$ of α to S (which is a homomorphism). Thus $S^\alpha \leq \text{Im } \alpha$. Conversely suppose that $T \leq \text{Im } \alpha$ and define $T^* = \{x \in G | x^\alpha \in T\}$; this is the *preimage* (or *inverse image*) of T. It is evident from the definition that $T^* \leq G$ and $(T^*)^\alpha = T$; notice also that T^* contains Ker α. Utilizing this notation it is easy to describe the subgroups of Im α.

1.4.6. *The functions $S \mapsto S^\alpha$ and $T \mapsto T^*$ are mutually inverse bijections between the set of subgroups of G that contain* Ker α *and the set of subgroups of* Im α. *A corresponding statement holds for normal subgroups.*

Proof. We have already observed that $(T^*)^\alpha = T$. Let $x \in (S^\alpha)^*$; then $x^\alpha = s^\alpha$ for some $s \in S$ and $xs^{-1} \in \text{Ker } \alpha \leq S$, so $x \in S$ and $(S^\alpha)^* \leq S$. Conversely $S \leq (S^\alpha)^*$ by the definition, so $(S^\alpha)^* = S$, which establishes the first part. Finally $S \lhd G$ implies that $S^\alpha \lhd \text{Im } \alpha$ and $T \lhd \text{Im } \alpha$ implies that $T^* \lhd G$, whence the second part follows. □

Specializing to the case of the natural homomorphism $G \to G/N$, one finds that *the subgroups of G/N are of the form S/N where $N \leq S \leq G$, with a like statement for normal subgroups.*

Direct Products

There are many ways of constructing a group from a given family of groups, the simplest of these constructions being the direct product.

Let $\{G_\lambda | \lambda \in \Lambda\}$ be a given set of groups. The *cartesian* (or *unrestricted direct*) *product*,

$$C = \underset{\lambda \in \Lambda}{\text{Cr}}\ G_\lambda,$$

is the group whose underlying set is the set product of the G_λ's, that is, the set of all "vectors" (g_λ) with λ-component g_λ in G_λ, and whose group operation is defined by multiplication of components: thus

$$(g_\lambda)(h_\lambda) = (g_\lambda h_\lambda),$$

$g_\lambda, h_\lambda \in G_\lambda$. Of course the identity element of C is to be (1_λ) and $(g_\lambda)^{-1} = (g_\lambda^{-1})$. It is an easy matter to check the validity of the group axioms.

The subset of all (g_λ) such that $g_\lambda = 1_\lambda$ for *almost all* λ, that is, with finitely many exceptions, is called the *external direct product*,

$$D = \underset{\lambda \in \Lambda}{\mathrm{Dr}}\, G_\lambda.$$

The G_λ are the *direct factors*. Clearly D is a subgroup of C; in fact it is even a normal subgroup. In case $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$, a finite set, we write

$$D = G_{\lambda_1} \times G_{\lambda_2} \times \cdots \times G_{\lambda_n}.$$

Of course $C = D$ in this case. Should the groups G_λ be written additively, we shall speak of the *direct sum* of the G_λ, and write

$$G_{\lambda_1} \oplus G_{\lambda_2} \oplus \cdots \oplus G_{\lambda_n}$$

instead of $G_{\lambda_1} \times G_{\lambda_2} \times \cdots \times G_{\lambda_n}$.

For each λ in Λ we define a function $\iota_\lambda\colon G_\lambda \to C$ by agreeing that $g_\lambda^{\iota_\lambda}$ shall be the vector whose λ-component is g_λ and whose other components are identity elements. Then ι_λ is a monomorphism with image $\bar{G}_\lambda$, a normal subgroup of C contained in D. Of course $\bar{G}_\lambda \simeq G_\lambda$. If $(g_\lambda) \in D$ and $g_{\lambda_1}, \ldots, g_{\lambda_k}$ are its nontrivial components, then clearly $(g_\lambda) = g_{\lambda_1}^{\iota_{\lambda_1}} \cdots g_{\lambda_k}^{\iota_{\lambda_k}}$, so that

$$D = \langle \bar{G}_\lambda | \lambda \in \Lambda \rangle.$$

It is also clear from the definition that

$$\bar{G}_\lambda \cap \langle \bar{G}_\mu | \mu \in \Lambda, \mu \neq \lambda \rangle = 1$$

for all λ.

Internal Direct Products

Suppose that H is a group with a family of normal subgroups $\{H_\lambda | \lambda \in \Lambda\}$ having the properties of the $\bar{G}_\lambda$ above, that is to say

$$H = \langle H_\lambda | \lambda \in \Lambda \rangle \qquad \text{and} \qquad H_\lambda \cap \langle H_\mu | \mu \in \Lambda, \mu \neq \lambda \rangle = 1.$$

Then H is called the *internal direct product* of the H_λ, which we shall write as $H = \mathrm{Dr}^{(\mathrm{i})}{}_{\lambda \in \Lambda} H_\lambda$.

Observe that elements of H which lie in different H_λ's commute. For if $x \in H_\lambda$, $y \in H_\mu$ and $\lambda \neq \mu$, then $x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) = (x^{-1}y^{-1}x)y \in H_\lambda \cap H_\mu = 1$; hence $xy = yx$.

Using this fact it is simple to prove that the mapping which assigns to an element of the external direct product the product of all its components is an isomorphism from $\mathrm{Dr}_{\lambda \in \Lambda} H_\lambda$ to $\mathrm{Dr}^{(\mathrm{i})}{}_{\lambda \in \Lambda} H_\lambda$.

We can sum up our conclusions about the relationship between internal and external direct products as follows.

1.4.7.

(i) *If* $\{G_\lambda | \lambda \in \Lambda\}$ *is a family of groups, the external direct product* $\mathrm{Dr}_{\lambda\in\Lambda} G_\lambda$ *is equal to the internal direct product* $\mathrm{Dr}^{(i)}{}_{\lambda\in\Lambda} \overline{G}_\lambda$ *where* $\overline{G}_\lambda$ *is the image of* $\iota_\lambda: G_\lambda \to \mathrm{Cr}_{\lambda\in\Lambda} G_\lambda$.
(ii) *Conversely the internal direct product* $\mathrm{Dr}^{(i)}{}_{\lambda\in\Lambda} H_\lambda$ *of a family of normal subgroups of a group is isomorphic with the external direct product* $\mathrm{Dr}_{\lambda\in\Lambda} H_\lambda$.

In the light of 1.4.7 we shall usually identify x in G_λ with x^{ι_λ} in $\overline{G}_\lambda$, so that $G_\lambda = \overline{G}_\lambda$ and internal and external direct products coincide.

The following characterization of the direct product is sometimes useful.

1.4.8. *Let* $\{G_\lambda | \lambda \in \Lambda\}$ *be a family of normal subgroups of a group G. Then G is the direct product of the* G_λ*'s if and only if*:

(i) *elements belonging to different* G_λ*'s commute*; *and*
(ii) *every element of G has a unique expression as a product of elements from distinct* G_λ*'s.*

Proof. Assume that G is the direct product of the G_λ's. Since the latter generate G, we can write any element x in the form $x = x_{\lambda_1} \cdots x_{\lambda_k}$ where $1 \neq x_{\lambda_i} \in G_{\lambda_i}$, the λ_i are distinct and $k \geq 0$: moreover, the order of the x_{λ_i} is immaterial. If $x = y_{\mu_1} \cdots y_{\mu_e}$ is another such expression for x and $\mu_1 \neq \lambda_i$ for all i, then $y_{\mu_1} \in G_{\mu_1} \cap \langle G_\lambda | \lambda \in \Lambda, \lambda \neq \mu_1 \rangle$, which is trivial. It is now easy to see that (i) and (ii) hold. Conversely, if these conditions are fulfilled, the intersection of G_λ and $\langle G_\mu | \mu \in \Lambda, \mu \neq \lambda \rangle$ must be trivial by the requirement of uniqueness. □

Direct Limits

Let Λ be a partially ordered set which is *directed*; this means that given λ and μ in Λ there exists a ν in Λ such that $\lambda \leq \nu$ and $\mu \leq \nu$. Suppose that we have a family of groups G_λ, $\lambda \in \Lambda$, and homomorphisms $\alpha_\lambda^\mu: G_\lambda \to G_\mu$ where $\lambda \leq \mu$, satisfying the following requirements:

(i) α_λ^λ is the identity map on G_λ;
(ii) $\alpha_\lambda^\mu \alpha_\mu^\nu = \alpha_\lambda^\nu$ whenever $\lambda \leq \mu \leq \nu$.

Then the set $\mathbf{D} = \{G_\lambda, \alpha_\lambda^\mu | \lambda \leq \mu \in \Lambda\}$ is called a *direct system* of groups.

We shall how to construct a group

$$D = \varinjlim_{\lambda\in\Lambda} G_\lambda$$

and homomorphisms

$$\theta_\lambda: G_\lambda \to D.$$

The resulting set $\{D, \theta_\lambda | \lambda \in \Lambda\}$ is called the *direct limit* of the direct system **D**. The idea here is that in **D** an element g_λ of G_λ is to be identified with all its images $g_\lambda^{\alpha_\lambda^\mu}$.

We shall assume that the groups G_λ are disjoint, so that $G_\lambda \cap G_\mu = \emptyset$ if $\lambda \neq \mu$. There is no real loss of generality here since G_λ can be replaced by a suitable isomorphic copy. In the sequel g_λ will always denote an element of G_λ.

We introduce a relation $\sim$ on the set-theoretic union

$$U = \bigcup_{\lambda \in \Lambda} G_\lambda,$$

defining $g_\lambda \sim \bar{g}_\mu$ to mean that $g_\lambda^{\alpha_\lambda^\nu} = \bar{g}_\mu^{\alpha_\mu^\nu}$ for some $\nu \geq \lambda, \mu$. Notice that ν here can be replaced by any $\rho \geq \nu$, as may be seen by applying α_ν^ρ to both sides of the equation and appealing to property (ii). It is easy to verify with the aid of the two defining properties that $\sim$ is an equivalence relation on U.

Let $[g_\lambda]$ be the equivalence class containing g_λ and denote by D the set of all equivalence classes. We wish to make D into a group. Suppose that $g_\lambda \sim \bar{g}_{\bar{\lambda}}$ and $g_\mu \sim \bar{g}_{\bar{\mu}}$. Then we can find ν in Λ satisfying $\nu \geq \lambda, \bar{\lambda}, \mu, \bar{\mu}$ and such that $g_\lambda^{\alpha_\lambda^\nu} = \bar{g}_{\bar{\lambda}}^{\alpha_{\bar{\lambda}}^\nu}$ and $g_\mu^{\alpha_\mu^\nu} = \bar{g}_{\bar{\mu}}^{\alpha_{\bar{\mu}}^\nu}$. Hence $g_\lambda^{\alpha_\lambda^\nu} g_\mu^{\alpha_\mu^\nu} = \bar{g}_{\bar{\lambda}}^{\alpha_{\bar{\lambda}}^\nu} \bar{g}_{\bar{\mu}}^{\alpha_{\bar{\mu}}^\nu}$ and it is meaningful to define the product by

$$[g_\lambda][g_\mu] = [g_\lambda^{\alpha_\lambda^\nu} g_\mu^{\alpha_\mu^\nu}]$$

where $\nu \geq \lambda, \mu$. The directedness of the set and the definition of equivalence ensure that there is no dependence on ν here.

It is easy to check the validity of the group axioms: of course $1_D = [1_{G_\lambda}]$ and $[g_\lambda]^{-1} = [g_\lambda^{-1}]$. The homomorphism θ_λ is just $g_\lambda \mapsto [g_\lambda]$.

The essential properties of the direct limit for our purposes are these.

1.4.9. *Let $\bar{G}_\lambda$ be the image of θ_λ: $G_\lambda \to D$.*

(i) $D = \bigcup_{\lambda \in \Lambda} \bar{G}_\lambda$.
(ii) $\bar{G}_\lambda \leq \bar{G}_\mu$ *whenever* $\lambda \leq \mu$.
(iii) *If all the α_λ^μ are monomorphisms, then the θ_λ are monomorphisms, so that $G_\lambda \simeq \bar{G}_\lambda$.*

Proof. (i) is immediate.

(ii) $[g_\lambda] = [g_\lambda^{\alpha_\lambda^\mu}] \in \bar{G}_\mu$.

(iii) If $g_\lambda^{\theta_\lambda} = 1$, then $[g_\lambda] = 1 = [1_\lambda]$. Hence $g_\lambda^{\alpha_\lambda^\mu} = 1_\mu$ for some $\mu \geq \lambda$. Consequently $g_\lambda = 1$. □

A special case of the direct limit will be of particular interest to us. Let there be given a sequence of groups $G_1, G_2, \ldots$ and monomorphisms σ_i: $G_i \to G_{i+1}$. Defining α_i^j to be $\sigma_i \sigma_{i+1} \cdots \sigma_{j-1}$ if $i < j$, we obtain a direct system $\{G_i, \alpha_i^j\}$. The direct limit group D is the union of the chain of subgroups

$$\bar{G}_1 \leq \bar{G}_2 \leq \cdots$$

and $G_i \simeq \bar{G}_i$. Thus whenever we have such a sequence of groups G_i, it is possible to think of all the groups as being contained in or *embedded* in a larger group.

Finally an important example. Let $G_i = \langle x_i \rangle$ be a cyclic group of order p^i where p is a fixed prime. Define a monomorphism $\sigma_i: G_i \to G_{i+1}$ by $x_i^{\sigma_i} = x_{i+1}^p$. The limit of the direct system is an infinite abelian p-group which is the union of a chain of cyclic p-groups of orders $p, p^2, \ldots$. This group is called a *Prüfer*† *group of type* p^∞. It plays an important part in the theory of infinite abelian groups, as we shall see in Chapter 4.

Exercises 1.4

1. If G is an n-generator group and H is finite, prove that $|\mathrm{Hom}(G, H)| \leq |H|^n$.

2. Prove that a finitely generated group has only a finite number of subgroups of given finite index.

*3. If $H \lhd K \leq G$ and θ is a homomorphism from G, then $H^\theta \lhd K^\theta$. Deduce that $HN \lhd KN$ whenever $N \lhd G$.

4. If H is abelian, $\mathrm{Hom}(G, H)$ is an abelian group if the group operation is defined by $g^{\alpha+\beta} = g^\alpha g^\beta$.

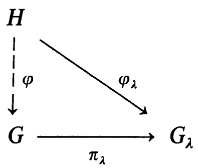
5. If G and H are groups with coprime finite orders, then $\mathrm{Hom}(G, H)$ contains only the zero homomorphism.

6. Let $N \lhd G$. Show that G/N is simple if and only if N is a maximal (proper) normal subgroup of G.

7. Prove that $(H \times K) \times L \simeq H \times K \times L \simeq H \times (K \times L)$.

8. An abelian group of exponent p is a direct product of cyclic groups of order p—such groups are called *elementary abelian p-groups*. [*Hint*: Regard the group as a vector space over $GF(p)$.]

*9. (*The mapping property of the cartesian product*). Let $G = \mathrm{Cr}_{\lambda \in \Lambda} G_\lambda$ and define the projections $\pi_\lambda: G \to G_\lambda$ by setting x^{π_λ} equal to the λ-component of x. Show that π_λ is a homomorphism. Let there be given a family of homomorphisms $\varphi_\lambda: H \to G_\lambda$ from some group H. Prove that there exists a unique homomorphism $\varphi: H \to G$ such that $\varphi\pi_\lambda = \varphi_\lambda$ for all λ. (This conclusion may be made more palatable by asserting that the diagrams



are *commutative*.)

† Heinz Prüfer (1896–1934).

*10. Prove that the mapping property in Exercise 1.4.9 characterizes the cartesian product in the following sense. Suppose that $\bar{G}$ is a group and $\bar{\pi}_\lambda: \bar{G} \to G_\lambda$ a family of homomorphisms such that whenever we are given homomorphisms $\varphi_\lambda: H \to G_\lambda$, there exists a *unique* homomorphism $\varphi: H \to \bar{G}$ such that $\varphi\bar{\pi}_\lambda = \varphi_\lambda$ for all λ. Then $\bar{G} \simeq \mathrm{Cr}_{\lambda \in \Lambda} G_\lambda$. *Remark*: This shows that the cartesian product is the product in the category of groups. The coproduct is the free product (see 6.2).

11. Show that $\mathbb{Q}$ is a direct limit of infinite cyclic groups.

12. Find some nonisomorphic groups that are direct limits of cyclic groups of orders $p, p^2, p^3, \dots$.

1.5. Endomorphisms and Automorphisms

Let G be a group and let $F(G)$ be the set of all functions from G to G. If $\alpha, \beta \in F(G)$, then $\alpha\beta \in F(G)$ where, of course, $x^{\alpha\beta} = (x^\alpha)^\beta$. Thus $F(G)$ is a set with an associative binary operation and an identity element, namely the identity function $1: G \to G$. Such an algebraic system is called a *monoid*.

There is a natural definition of the *sum* of two elements of $F(G)$, namely $x^{\alpha+\beta} = x^\alpha x^\beta$. Clearly addition is an associative operation. In fact $F(G)$ is a group with respect to addition: for the additive identity element is the zero homomorphism $0: G \to G$ and the inverse $-\alpha$ is given by $x^{-\alpha} = (x^\alpha)^{-1}$.

It is straightforward to verify the *left distributive law* $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$: however the *right distributive law* $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ does not hold in $F(G)$ in general.

As an additive group and a multiplicative monoid which satisfies the left distributive law, $F(G)$ is a type of algebraic system known as a left *near ring*.

Let End G denote the set of all endomorphisms of G; thus $\{0, 1\} \subseteq \text{End } G \subseteq F(G)$. If $\alpha, \beta \in \text{End } G$, then $\alpha\beta \in \text{End } G$, so that the End G is a multiplicative submonoid of $F(G)$. The sum $\alpha + \beta$ need not be an endomorphism, but in case it is, α and β are said to be *additive*.

1.5.1. *Let α, β be endomorphisms of a group G. Then $\alpha + \beta$ is an endomorphism if and only if every element of* Im α *commutes with every element of* Im β. *Moreover $\alpha + \beta = \beta + \alpha$ in this case.*

Proof. The equation $(xy)^{\alpha+\beta} = x^{\alpha+\beta}y^{\alpha+\beta}$ is equivalent to $y^\alpha x^\beta = x^\beta y^\alpha$. If we put $x = y$, this yields in particular $x^{\alpha+\beta} = x^{\beta+\alpha}$ and $\alpha + \beta = \beta + \alpha$. □

If $\alpha, \beta \in F(G)$ and $\gamma \in \text{End } G$, then $x^{(\alpha+\beta)\gamma} = (x^\alpha x^\beta)^\gamma = x^{\alpha\gamma+\beta\gamma}$, which shows that the right distributive law $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ is valid in this case. Should the group G be abelian, it follows from 1.5.1 that End G is a ring. In fact the converse is true: for if $1 + 1$ is an endomorphism, it is a consequence of 1.5.1 that G is abelian.

Automorphisms

If G is a group, an *automorphism* of G is an isomorphism from G to G. The set of automorphisms of G is denoted by

$$\text{Aut } G:$$

this, then, is the subset of elements of End G which possess multiplicative inverses. Aut G is a group with respect to functional composition since the inverse of $\alpha\beta$ in Aut G is $\beta^{-1}\alpha^{-1}$.

Suppose that $x, g \in G$ and write

$$x^g = g^{-1}xg:$$

this element is called the *conjugate* of x by g. Consider the function $g^\tau: G \to G$ defined by $(x)g^\tau = x^g$. Since $(xy)^g = x^g y^g$ and $g^\tau(g^{-1})^\tau = 1 = (g^{-1})^\tau g^\tau$, we see that $g^\tau \in \text{Aut } G$. We call g^τ *the inner automorphism of* G *induced by* g and write

$$\text{Inn } G$$

for the set of all inner automorphisms.

1.5.2. *If G is any group, the function $\tau: G \to \text{Aut } G$ defined by $(x)g^\tau = x^g$ is a homomorphism with image* Inn G *and kernel the set of elements that commute with every element of G.*

Proof. By definition $x^{(gh)^\tau} = (gh)^{-1}x(gh) = h^{-1}g^{-1}xgh = (x^{g^\tau})^{h^\tau}$, so $(gh)^\tau = g^\tau h^\tau$. Evidently $g^\tau = 1_{\text{Aut } G}$ is equivalent to $gx = xg$ for all $x \in G$. □

The kernel of τ is called the *center* of G and will be written ζG. Thus

$$\zeta G = \{x \in G \mid xg = gx \text{ for all } \quad g \in G\}.$$

1.5.3. *If G is any group, then $\zeta G \lhd G$ and $G/\zeta G \simeq$* Inn G.

This follows from 1.5.2 and the First Isomorphism Theorem (1.4.3).

1.5.4. *If G is a group and g^τ is the inner automorphism induced by g, then $\alpha^{-1}g^\tau\alpha = (g^\alpha)^\tau$ for all $\alpha \in$* Aut G. *Hence* Inn $G \lhd$ Aut G.

Proof. Let $g \in G$ and $\alpha \in \text{Aut } G$; then $\alpha^{-1}g^\tau\alpha$ maps x to $(g^{-1}x^{\alpha^{-1}}g)^\alpha = (g^\alpha)^{-1}xg^\alpha$, which shows that $\alpha^{-1}g^\tau\alpha = (g^\alpha)^\tau$. □

An automorphism of G which is not inner is called *outer*; the quotient group

$$\text{Out } G = (\text{Aut } G)/(\text{Inn } G)$$

is called the *outer automorphism group* of G, even although its elements are not automorphisms.

The Automorphism Group of a Cyclic Group

1.5.5. *Let G be a cyclic group.*

(i) *If G is infinite,* Aut G *consists of the identity automorphism and the automorphism $g \mapsto g^{-1}$. Thus* Aut G *is cyclic of order 2.*
(ii) *If G has finite order n, then* Aut G *consists of all automorphisms α_k: $g \mapsto g^k$ where $1 \leq k < n$ and $(k, n) = 1$: moreover the mapping $k + n\mathbb{Z} \mapsto \alpha_k$ is an isomorphism from $\mathbb{Z}_n^*$ (the multiplicative group of units of the ring $\mathbb{Z}_n$) to* Aut G. *In particular* Aut G *is abelian and has order $\varphi(n)$ where φ is Euler's function.*

Proof. Let $G = \langle x \rangle$ and let $\alpha \in \text{Aut } G$. Since $(x^n)^\alpha = (x^\alpha)^n$, the automorphism α is completely determined by x^α. Notice that x^α must generate G. If G is infinite, x and x^{-1} are the only generators, so $x^\alpha = x$ or x^{-1}. Both possibilities clearly give rise to automorphisms, so (i) is established.

Now let $|G| = n < \infty$. Since x^α must have order n, we conclude with the aid of 1.3.8 that $x^\alpha = x^k$ where $1 \leq k < n$ and $(k, n) = 1$. Conversely, given such an integer k, the mapping $g \mapsto g^k$ is an automorphism. The rest is clear. □

Semidirect Products

We describe next an exceedingly useful construction that is a generalization of the direct product of two groups.

Suppose that $N \lhd G$ and there is a subgroup H such that $G = HN$ and $H \cap N = 1$; then G is said to be the *internal semidirect product* of N and H; in symbols

$$G = H \ltimes N \qquad \text{or} \qquad G = N \rtimes H.$$

Each element of G has a *unique* expression of the form hn where $h \in H$ and $n \in N$. For example, the dihedral group D_{2n} is a semidirect product of a cyclic group of order n and a group of order 2. (See Exercise 1.3.17.) Conjugation in N by an element h of H yields an automorphism h^α of N and α: $h \mapsto h^\alpha$ is a homomorphism from H to Aut N. Observe that G is the direct product of H and N if and only if α is the zero homomorphism.

Conversely suppose that we are given two groups H and N, together with a homomorphism α: $H \to \text{Aut } N$. The *external semidirect product* $G = H \ltimes_\alpha N$ (or $N \rtimes_\alpha H$) is the set of all pairs (h, n), $h \in H$, $n \in N$, with the group operation

$$(h_1, n_1)(h_2, n_2) = (h_1 h_2, n_1^{h_2^\alpha} n_2):$$

the motivation here is, of course, the equation $(x_1 y_1)(x_2 y_2) = x_1 x_2 y_1^{x_2} y_2$, which holds in any group. The identity element is $(1_H, 1_N)$ and $(h, n)^{-1} = (h^{-1}, (n^{-1})^{(h^\alpha)^{-1}})$. We leave the reader to verify the associative law.

Let us consider the functions $h \mapsto (h, 1_N)$ and $n \mapsto (1_H, n)$. These are monomorphisms from H to G and N to G respectively. Writing H^* and N^* for their images we have, of course, $H \simeq H^*$ and $N \simeq N^*$. Since $(h, 1_N)(1_H, n) = (h, n)$, we have also $G = H^*N^*$, while it is clear that $H^* \cap N^* = 1$. Finally $(h, 1_N)^{-1}(1_H, n)(h, 1_N) = (1_H, n^{h^\alpha})$, which shows that $N^* \lhd G$ and G is the internal semidirect product of N^* and H^*. Notice that conjugation in N^* by $(h, 1_N)$ induces the automorphism h^α. Usually it is convenient not to distinguish between N and N^* and H and H^*, so that G can be thought of as the internal semidirect product of N and H. In the future we shall simply speak of *the* semidirect product $H \ltimes N$.

Characteristic and Fully-Invariant Subgroups

A subgroup H of a group G is said to be *fully-invariant* in G if $H^\alpha \leq H$ for all $\alpha \in \operatorname{End} G$, and *characteristic* in G if $H^\alpha \leq H$ for all $\alpha \in \operatorname{Aut} G$. Notice that if H is characteristic in G and $\alpha \in \operatorname{Aut} G$, then H^α must actually equal H since $H^\alpha \leq H$ and $H^{\alpha^{-1}} \leq H$.

1.5.6.

(i) *Fully-invariant subgroups are characteristic and characteristic subgroups are normal.*

(ii) *"Fully-invariant" and "characteristic" are transitive relations.* (*This is not true for normality.*)

(iii) *If H is characteristic in K and $K \lhd G$, then $H \lhd G$.*

Proof. (i) is clear and (ii) follows from the fact that the restriction of an endomorphism (automorphism) to a fully-invariant (characteristic) subgroup is an endomorphism (automorphism). To prove (iii) note that conjugation in K by $g \in G$ is an automorphism, so $H = g^{-1}Hg$. □

For example, *the center of a group is always characteristic*: if $x \in \zeta G$ and $\alpha \in \operatorname{Aut} G$, then $xg = gx$ yields $x^\alpha g^\alpha = g^\alpha x^\alpha$, which implies that $x^\alpha \in \zeta G$ because $G = G^\alpha$. In a certain sense dual to ζG is the *derived subgroup* G' generated by all *commutators* $[x, y] = x^{-1}y^{-1}xy$: since $[x, y]^\alpha = [x^\alpha, y^\alpha]$ whenever $\alpha \in \operatorname{End} G$, we see that *the derived subgroup is fully-invariant.* The center of a group is not in general fully-invariant (Exercise 1.5.9). Another example of a fully-invariant subgroup is G^n, the *subgroup generated by all* nth *powers of elements of* G.

Operator Groups

We introduce next a very useful generalization of the concept of a group. A *right operator group* is a triple (G, Ω, α) consisting of a group G, a set Ω

called the *operator domain* and a function $\alpha: G \times \Omega \to G$ such that $g \mapsto (g, \omega)\alpha$ is an endomorphism of G for each $\omega \in \Omega$. We shall write g^ω for $(g, \omega)\alpha$ and speak of the *Ω-group* G if the function α is understood. Thus an operator group is a group with a set of operators which act on the group like endomorphisms.

Since any group can be regarded as an operator group with empty operator domain, an operator group is a generalization of a group. The concept of a *left operator group* is defined in the obvious way.

It is possible to generalize to operator groups many of the concepts which have already been defined for groups. If G is an Ω-group, an *Ω-subgroup* of G is a subgroup H which is *Ω-admissible*, that is, such that $h^\omega \in H$ whenever $h \in H$ and $\omega \in \Omega$. Clearly every Ω-subgroup is itself an Ω-group. *The intersection of a set of Ω-subgroups is an Ω-subgroup.* This permits us to define *the Ω-subgroup generated by a nonempty subset X* as the intersection of all the Ω-subgroups containing X. This may be written

$$X^\Omega.$$

By the method of 1.3.3 it may be shown that X^Ω consists of all elements $(x_1^{\varepsilon_1})^{\omega_1} \cdots (x_r^{\varepsilon_r})^{\omega_r}$ where $x_i \in X$, $\varepsilon_i = \pm 1$, $r \geq 0$ and ω_i is a sequence of elements of Ω applied successively.

If N is a normal Ω-subgroup, the quotient group G/N becomes an *Ω-quotient group* if we define $(Ng)^\omega = Ng^\omega$. An *Ω-homomorphism* $\alpha: G \to H$ is a homomorphism between Ω-groups G and H such that

$$(g^\omega)^\alpha = (g^\alpha)^\omega$$

for all $g \in G$ and $\omega \in \Omega$. The set of all Ω-homomorphisms from G to H is written

$$\mathrm{Hom}_\Omega(G, H).$$

With these definitions it is possible to carry over to Ω-groups the theory of homomorphisms and quotient groups described in 1.4. Thus $\mathrm{Im}\,\alpha$ is an Ω-subgroup of G and $\mathrm{Ker}\,\alpha$ a normal Ω-subgroup of G. The isomorphism theorems for Ω-groups hold: here of course all homomorphisms are Ω-homomorphisms. For example: $G/\mathrm{Ker}\,\alpha \simeq^\Omega \mathrm{Im}\,\alpha$ where the sumbol $\simeq^\Omega$ means "Ω-isomorphic." We can also speak of *Ω-endomorphisms* (= Ω-homomorphisms from a group to itself) and *Ω-automorphisms* (= bijective Ω-endomorphisms). These form sets $\mathrm{End}_\Omega\, G$ and $\mathrm{Aut}_\Omega\, G$: clearly $\mathrm{End}_\Omega\, G \subseteq \mathrm{End}\, G$ and $\mathrm{Aut}_\Omega\, G \leq \mathrm{Aut}\, G$.

The reader is urged to prove the theorems about Ω-groups just mentioned: in all cases the proofs are close copies of the original ones.

Examples of Operator Groups

(i) If R is a ring and A is a right R-module, then A is a right R-operator group. Thus modules are particular instances of operator groups.

(ii) Let G be any group and let $\Omega = \text{End } G$. Then G is an Ω-group if we allow endomorphisms to operate on G in the natural way. An Ω-subgroup of G is simply a fully-invariant subgroup.

(iii) In the same way G is an operator group with respect to $\Omega = \text{Aut } G$. Here the Ω-subgroups are the characteristic subgroups.

(iv) Finally G is an operator group with respect to $\Omega = \text{Inn } G$. The Ω-subgroups are of course the normal subgroups of G. The Ω-endomorphisms are those that commute with every inner automorphism of G. Such endomorphisms are called *normal*. Notice that X^Ω is just the normal closure X^G.

From the foregoing discussion it is clear that the concept of an operator group unifies many previous ideas. There is also a definite advantage in proving results for operator groups rather than simply for groups. This is a point of view to which we shall give particular attention in Chapter 3.

Exercises 1.5

1. Let $\mathbb{Q}_p$ be the additive group of rational numbers of the form mp^n where $m, n \in \mathbb{Z}$ and p is a fixed prime. Describe End $\mathbb{Q}_p$ and Aut$\mathbb{Q}_p$.
2. The same question for $\mathbb{Q}$.
*3. Prove the isomorphism theorems for operator groups.
4. If $\alpha \in \text{Aut } G$ and $g \in G$, then g and g^α have the same orders.
5. Prove that Aut $S_3 \simeq S_3$.
6. Prove that Aut $D_8 \simeq D_8$ and yet D_8 has outer automorphisms.
7. If $G/\zeta G$ is cyclic, then G is abelian.
*8. Prove that $\zeta(\text{Dr}_\lambda G_\lambda) = \text{Dr}_\lambda \zeta G_\lambda$.
9. The center of the group $A_4 \times \mathbb{Z}_2$ is not fully-invariant.
10. Let $G = G_1 \times G_2 \times \cdots \times G_n$ where the G_i are abelian groups. Prove that Aut G is isomorphic with the group of all invertible $n \times n$ matrices whose (i, j) entries belong to Hom(G_i, G_j), the usual matrix product being the group operation.
*11. Prove that
$$\text{Aut}(\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}) \simeq GL(n, \mathbb{Z}) \quad \text{and} \quad \text{Aut}(\underbrace{\mathbb{Z}_{p^m} \oplus \cdots \oplus \mathbb{Z}_{p^m}}_{n}) \simeq GL(n, \mathbb{Z}_{p^m}).$$
12. Give an example of an abelian group and a nonabelian group with isomorphic automorphism groups.
*13. Let $G = \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}}$ where $n_1 < n_2 < \cdots < n_k$. Prove that there exists a chain of characteristic subgroups $1 = G_0 < G_1 < \cdots < G_t = G$ such that $|G_{i+1} : G_i| = p$ and $t = \sum_{i=1}^k n_i$. Deduce that $|\text{Aut } G| = (p-1)p^r$ for some r.
14. Prove that $\text{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_4) \simeq D_8$.
15. Show that no group can have its automorphism group cyclic of odd order > 1.

*16. If G has order $n > 1$, then $|\text{Aut } G| \leq \prod_{i=0}^{k}(n - 2^i)$ where $k = [\log_2(n-1)]$. [*Hint*: Use Exercise 1.3.4.]

17. If an automorphism fixes more than half of the elements of a finite group, then it is the identity automorphism.

18. Let α be an automorphism of a finite group G which inverts more than three quarters of the elements of G. Prove that $g^\alpha = g^{-1}$ for all $g \in G$ and that G is abelian. [*Hint*: Let $S = \{g \in G | g^\alpha = g^{-1}\}$, and show that $|S \cap xS| > \frac{1}{2}|G|$ where $x \in S$].

1.6. Permutation Groups and Group Actions

If X is a nonempty set, a subgroup G of the symmetric group Sym X is called a *permutation group* on X. The *degree* of the permutation group is the cardinality of X.

Two *points* (i.e., elements) x and y of X are said to be *G-equivalent* if there exists a permutation π in G such that $x\pi = y$. It is easy to see that this relation is an equivalence relation on X. The equivalence classes are known as *G-orbits*, the orbit containing x being of course $\{x\pi | \pi \in G\}$. Thus *X is partitioned into G-orbits.*

The permutation group G is called *transitive* if, given any pair of elements x, y of X, there exists a permutation π in G such that $x\pi = y$. Thus G is transitive if and only if there is exactly one G-orbit, namely X itself. For example the 4-group $\{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ is transitive but its subgroup $\{1, (1, 2)(3, 4)\}$ is not.

If Y is a nonempty subset of X, the *stabilizer* of Y in G

$$\text{St}_G(Y)$$

is the set of permutations in G that leave fixed every element of Y. Of course $\text{St}_G(x)$ stands for $\text{St}_G(\{x\})$. The permutation group G is said to be *semiregular* if $\text{St}_G(x) = 1$ for all x in X. A *regular* permutation group is one that is both transitive and semiregular.

We record next the most elementary properties of permutation groups.

1.6.1. *Let G be a permutation group on a set X.*

(i) *Let $x \in X$. Then the mapping $\text{St}_G(x)\pi \mapsto x\pi$ is a bijection between the set of right cosets of $\text{St}_G(x)$ and the orbit of x. Hence the latter has cardinality $|G : \text{St}_G(x)|$.*
(ii) *If G is transitive, then $|G| = |X| \cdot |\text{St}_G(x)|$ for all x in X.*
(iii) *If G is regular, then $|G| = |X|$.*

Proof. It is clear that the mapping in (i) is well-defined and surjective. If $x\pi = x\pi'$ where $\pi, \pi' \in G$, then $\pi(\pi')^{-1} \in \text{St}_G(x)$ and $\text{St}_G(x)\pi = \text{St}_G(x)\pi'$. All the remaining statements now follow. □

1.6.2. *Let G be a permutation group on a set X. If $x \in X$ and $\pi \in G$, then* $\mathrm{St}_G(x\pi) \equiv \pi^{-1} \mathrm{St}_G(x)\pi$.

Proof. An element σ of G fixes $x\pi$ if and only if $\pi\sigma\pi^{-1}$ fixes x, which is equivalent to $\sigma \in \pi^{-1} \mathrm{St}_G(x)\pi$. □

This has the following easy but important corollary:

1.6.3. *Let G be a transitive permutation group on a set X. If G is abelian, it is regular.*

Proof. Let x be any element of X. If $\pi \in G$, then $(\mathrm{St}_G(x))^\pi = \mathrm{St}_G(x\pi)$ by 1.6.2. But $\mathrm{St}_G(x) \lhd G$ because G is abelian. Hence $\mathrm{St}_G(x) = \mathrm{St}_G(x\pi)$ for all π in G. Since G is transitive, it follows that a permutation fixing x will fix every element of X. Hence $\mathrm{St}_G(x) = 1$. □

Similar Permutation Groups

Similarity is a way of comparing permutation groups just as isomorphism compares abstract groups. Let G and H be permutation groups on sets X and Y respectively. A *similarity* from G to H is a pair (α, β) consisting of an isomorphism $\alpha: G \to H$ and a bijection $\beta: X \to Y$ which are related by the rule

$$\pi\beta = \beta\pi^\alpha \qquad (\pi \in G).$$

When $X = Y$, this says that $\pi^\alpha = \beta^{-1}\pi\beta$ where now $\beta \in \mathrm{Sym}\, X$. Thus two permutation groups G and H on X are similar if and only if some β in $\mathrm{Sym}\, X$ conjugates G into H. Clearly if $|X| = |Y|$, then $\mathrm{Sym}\, X$ and $\mathrm{Sym}\, Y$ are similar.

Similarity is a stronger relation than isomorphism. For example $G = \langle(1, 2)(3, 4)\rangle$ and $H = \langle(1, 2)(3)(4)\rangle$ are isomorphic as abstract groups, but they are not similar as permutation groups (why not?).

The Wreath Product of Permutation Groups

Let H and K be permutation groups acting on sets X and Y respectively. We shall describe a very important way of constructing a new permutation group called the wreath product of H and K. This is to act on the set product $Z = X \times Y$.

If $\gamma \in H$, $y \in Y$, and $\kappa \in K$, define permutations $\gamma(y)$ and κ^* of Z by the rules

$$\gamma(y): \begin{cases} (x, y) \mapsto (x\gamma, y), \\ (x, y_1) \mapsto (x, y_1) \quad \text{if } y_1 \neq y, \end{cases}$$

and

$$\kappa^*: (x, y) \mapsto (x, y\kappa).$$

One verifies quickly that $(\gamma^{-1})(y) = (\gamma(y))^{-1}$ and $(\kappa^{-1})^* = (\kappa^*)^{-1}$, so that $\gamma(y)$ and κ^* are in fact permutations. The functions $\gamma \mapsto \gamma(y)$, with y a fixed element of Y, and $\kappa \mapsto \kappa^*$ are monomorphisms from H and K to $\operatorname{Sym} Z$: let their images be $H(y)$ and K^*, respectively. Then the *wreath product* of H and K is the permutation group on Z generated by K^* and all the $H(y)$, $y \in Y$. This is written

$$H \wr K = \langle H(y), K^* | y \in Y \rangle.$$

Observe that $(\kappa^*)^{-1}\gamma(y)\kappa^*$ maps $(x, y\kappa)$ to $(x\gamma, y\kappa)$ and fixes (x_1, y_1) if $y_1 \neq y\kappa$. Hence by definition

$$(\kappa^*)^{-1}\gamma(y)\kappa^* = \gamma(y\kappa) \qquad \text{and} \qquad (\kappa^*)^{-1}H(y)\kappa^* = H(y\kappa). \tag{1}$$

In addition notice that when $y \neq y_1$ the permutations $\gamma(y)$ and $\gamma_1(y_1)$ cannot move the same element of Z. It follows that the $H(y)$'s generate their direct product, B say; the latter is called the *base group* of the wreath product:

$$B = \operatorname*{Dr}_{y \in Y} H(y).$$

According to (1) conjugation by an element κ^* of K^* permutes the direct factors $H(y)$ in the same way as κ permutes the elements of Y. Since elements of K^* and B cannot move the same element of Z, we must have $K^* \cap B = 1$. Also of course $B \lhd W$ and $W = K^*B$. Thus *W is the semidirect product of B by K^* in which the automorphism of B produced by an element of K^* is given by* (1). For simplicity of notation let us agree to identify κ^* with κ, so that $K^* = K$.

We record two basic properties of wreath products.

1.6.4.

(i) *If H and K are transitive, so is $H \wr K$.*
(ii) *Let L be a permutation group on U. Let $\beta: (X \times Y) \times U \to X \times (Y \times U)$ be the bijection $((x, y), u) \mapsto (x, (y, u))$ and let α be the function $\tau \mapsto \beta^{-1}\tau\beta$. Then (α, β) is a similarity from $(H \wr K) \wr L$ to $H \wr (K \wr L)$.*

Proof. (i) Let (x, y) and (x', y') belong to $Z = X \times Y$. By transitivity there exist $\gamma \in H$ and $\kappa \in K$ such that $x' = x\gamma$ and $y' = y\kappa$. Then $\kappa\gamma(y')$ maps (x, y) to $(x, y') \cdot \gamma(y') = (x', y')$, whence $H \wr K$ is transitive.

(ii) Let $S = (X \times Y) \times U$ and $T = X \times (Y \times U)$. In the first place the map $\alpha: \tau \mapsto \beta^{-1}\tau\beta$ is clearly an isomorphism from $\operatorname{Sym} S$ to $\operatorname{Sym} T$. Let us consider the image of $(H \wr K) \wr L$ under this isomorphism. If $\gamma \in H$, then $(\gamma(y))(u)$ maps $((x, y), u)$ to $((x\gamma, y), u)$ and fixes $((x, y_1), u_1)$ if $u_1 \neq u$ or $y_1 \neq y$: hence $\beta^{-1}(\gamma(y)(u))\beta$ maps $(x, (y, u))$ to $(x\gamma, (y, u))$ and fixes $(x, (y_1, u_1))$ if $(y_1, u_1) \neq (y, u)$. Therefore $\beta^{-1}(\gamma(y)(u))\beta = \gamma((y, u))$. Also if

$\kappa \in K$ and $\lambda \in L$, then $\beta^{-1}(\kappa(u))\beta = \kappa^*(u)$ and $\beta^{-1}\lambda\beta = \lambda^*$ where * indicates that the permutation is to be formed in $H \sim (K \sim L)$. Hence α maps $(H \sim K) \sim L$ onto $H \sim (K \sim L)$, and (α, β) is a similarity. □

The second part of 1.6.4 asserts that *to within similarity the wreath product is an associative operation.*

Group Actions and Permutation Representations

Let G be a group and X a nonempty set. By a *right action* of G on X is meant a function $\rho: X \times G \to X$ such that $(x, g_1g_2)\rho = ((x, g_1)\rho, g_2)\rho$ and $(x, 1_G)\rho = x$. It is more suggestive to write xg instead of $(x, g)\rho$, so that the defining equations become

$$x(g_1g_2) = (xg_1)g_2 \qquad \text{and} \qquad x1_G = x \qquad (x \in X, g_i \in G). \tag{2}$$

A *left action* of G on X is defined analogously as a function $\lambda: G \times X \to X$ such that $(g_1g_2, x)\lambda = (g_1, (g_2, x)\lambda)\lambda$ and $(1_G, x)\lambda = x$ or $(g_1g_2)x = g_1(g_2x)$ and $1_Gx = x$ with improved notation.

Let us consider a right action $(x, g) \mapsto xg$ of G on X. For a fixed element g of G the mapping $x \mapsto xg$ is a permutation of X: for it has as its inverse the mapping $x \mapsto xg^{-1}$, as we can see from (2). Call this permutation g^γ. Then $(g_1g_2)^\gamma$ maps x to $x(g_1g_2)$, as does $g_1^\gamma g_2^\gamma$. Hence $(g_1g_2)^\gamma = g_1^\gamma g_2^\gamma$. So the group action determines a homomorphism $\gamma: G \to \text{Sym } X$.

Conversely let γ be any homomorphism from G to Sym X—such a function is called a *permutation representation* of G on X. Then the mapping $(x, g) \mapsto xg^\gamma$ is a right action of G on X. Thus we have constructed a map from right actions of G on X to permutation representations of G on X, and also a map in the opposite direction. Clearly these are inverse mappings.

All of this can be done with left actions but a little care must be exercised. If $(g, x) \mapsto gx$ is a left action of G on X, the corresponding representation of G on X is γ where g^γ maps x to $g^{-1}x$: without this inverse we would not obtain a homomorphism.

1.6.5. *Let G be a group and X a nonempty set.*

(i) *There is a bijection between right actions of G on X and permutation representations of G on X in which the action $(x, g) \mapsto xg$ corresponds to the permutation representation $g \mapsto (x \mapsto xg)$.*
(ii) *There is a bijection between left actions of G on X and permutation representations of G on X in which the action $(g, x) \mapsto gx$ corresponds to the representation $g \mapsto (x \mapsto g^{-1}x)$.*

In view of this result we shall use the languages of group actions and of permutation representations interchangeably. In particular the following definitions apply to actions as well as to permutation representations.

Let $\gamma: G \to \operatorname{Sym} X$ be a permutation representation of G on X. The cardinality of X is known as the *degree* of the representation. Next γ is called *faithful* if $\operatorname{Ker} \gamma = 1$, so that G is isomorphic with a group of permutations of X. Also γ is said to be *transitive* if $\operatorname{Im} \gamma$ is a transitive permutation group. By an *orbit* of G we mean one of $\operatorname{Im} \gamma$. Finally the *stabilizer* of $x \in X$ in G is $\{g \in G \mid xg^{\gamma} = x\}$, and γ is regular if it is transitive and all stabilizers are trivial. It should be noted that 1.6.1 remains true when G merely acts on X.

Permutation Representations on Sets of Cosets

There are several natural ways of representing a group as a permutation group; one of the most useful arises when the group is allowed to act by right multiplication on the right cosets of a subgroup.

1.6.6. *Let H be a subgroup of a group G and let $\mathscr{R}$ be the set of all right cosets of H. For each g in G define $g^{\rho} \in \operatorname{Sym} \mathscr{R}$ by $g^{\rho}: Hx \mapsto Hxg$. Then $\rho: G \to \operatorname{Sym} \mathscr{R}$ is a transitive permutation representation of G on $\mathscr{R}$ with kernel H_G, the core of H in G.*

Proof. $(g^{-1})^{\rho} = (g^{\rho})^{-1}$, so $g^{\rho} \in \operatorname{Sym} \mathscr{R}$ and $\rho: G \to \operatorname{Sym} \mathscr{R}$ is plainly a homomorphism. Since $Hx = (Hg)g^{-1}x = (Hg)(g^{-1}x)^{\rho}$, we see that ρ is transitive. Finally $g^{\rho} = 1$ if and only if $Hxg = Hx$ for all x, that is,

$$g \in \bigcap_{x \in G} x^{-1}Hx = H_G. \qquad \square$$

Equivalent Permutation Representations

Two permutation representations of a group $\gamma: G \to \operatorname{Sym} X$ and $\delta: G \to \operatorname{Sym} Y$ are said to be *equivalent* if there exists a bijection $\beta: X \to Y$ such that

$$\beta g^{\delta} = g^{\gamma}\beta$$

for all g in G. When $X = Y$, the equivalence of γ and δ can be restated in the form $g^{\delta} = \beta^{-1}g^{\gamma}\beta$ for some $\beta \in \operatorname{Sym} X$.

The importance of the permutation representation on the right cosets of a subgroup is brought out by the following fact.

1.6.7. *Let G be a group and let $\gamma: G \to \operatorname{Sym} X$ be a transitive permutation representation of G on a set X. Then γ is equivalent to the standard permutation representation of G on the right cosets of one of its subgroups.*

Proof. Choose an element x of X and fix it. Let $H = \operatorname{St}_G(x)$ and write $\mathscr{R}$ for the set of right cosets of H in G. Then in fact γ is equivalent to the natural permutation representation δ on $\mathscr{R}$. To establish this we shall find a bijec-

tion $\beta: \mathscr{R} \rightarrow X$ such that $g_1^\delta \beta = \beta g_1^\gamma$ for all g_1 in G. Take β to be the map $Hg \mapsto xg^\gamma$. Note that β is well-defined since $x(hg)^\gamma = xg^\gamma$ if $h \in H$: also β is surjective by transitivity of γ, while it is injective because $xg^\gamma = xg_1^\gamma$ implies that $gg_1^{-1} \in H$ and $Hg = Hg_1$.

Finally we verify that $g_1^\delta \beta$ sends Hg to $(Hgg_1)\beta = x(gg_1)^\gamma$, while βg_1^γ sends Hg to $xg^\gamma g_1^\gamma = x(gg_1)^\gamma$. □

There is of course a natural permutation representation of G on the set of *left* cosets of a given subgroup H, given by $g^\gamma: xH \rightarrow g^{-1}xH$. Here the inverse is necessary to ensure that γ is a homomorphism.

A particularly important case occurs when $H = 1$ and G is represented by permutations of its underlying set via left or right multiplication. Then we obtain the so-called *left regular* and *right regular* permutation representations of G: these are λ and ρ where

$$g^\lambda: x \mapsto g^{-1}x \qquad \text{and} \qquad g^\rho: x \mapsto xg.$$

By 1.6.6 both λ and ρ are faithful: it is easy to see that they are also regular.

The following is a consequence of the existence of these representations.

1.6.8 (Cayley's Theorem). *If G is any group, it is isomorphic with a subgroup of* Sym G,

The idea which underlies the permutation representation on cosets has numerous applications.

1.6.9. *If H is a subgroup with finite index n in a group G, then the core H_G has finite index dividing $n!$.*

Proof. By 1.6.6 the group G/H_G is isomorphic with a subgroup of S_n. □

1.6.10. *Suppose that H is a subgroup with index p in a finite group G where p is the smallest prime dividing $|G|$. Then $H \lhd G$. In particular a subgroup of index 2 is always normal.*

Proof. By 1.6.9 the order of G/H_G divides $p!$, whence $|G:H_G| = 1$ or p since no smaller prime than p can divide $|G:H_G|$. But $H_G \leq H$ and $|G:H| = p$, so $H = H_G \lhd G$. □

1.6.11. *Let H be a subgroup of finite index in a finitely generated group G. Then H is finitely generated.*

Proof. Let X be a finite set of generators of G and let $\{1 = t_1, t_2, \ldots, t_i\}$ be a right transversal to H in G. If $g \in G$, then $Ht_jg = Ht_{(j)g}$ where $j \mapsto (j)g$ is a permutation of $\{1, 2, \ldots, i\}$. Hence

$$t_jg = h(j, g)t_{(j)g}, \tag{3}$$

where $h(j, g) \in H$. Let $a \in H$ and write $a = y_1 \cdots y_k$ where $y_l \in X \cup X^{-1}$. By repeated application of (3) we obtain

$$a = t_1 a = h(1, y_1)h((1)y_1, y_2) \cdots h((1)y_1 \cdots y_{k-1}, y_k)t_{(1)a}.$$

But $Ht_{(1)a} = Ht_1 a = H$ since $t_1 = 1$: thus $t_{(1)a} = 1$. It follows that the $h(j, y)$, $1 \leq j \leq i$, $y \in X \cup X^{-1}$, generate H. □

However subgroups of finitely generated groups are not always finitely generated (Exericse 1.6.15).

The Holomorph

Let $\lambda: G \to \text{Sym}\, G$ and $\rho: G \to \text{Sym}\, G$ be the left and right regular representations of a group G. Then G^λ and G^ρ are subgroups of Sym G, as is Aut G. Now $g^\lambda g^\rho$ maps x to $g^{-1}xg$, so $g^\lambda g^\rho$ is just g^τ, the inner automorphism induced by g. Consequently

$$\langle G^\lambda, \text{Aut}\, G\rangle = \langle G^\rho, \text{Aut}\, G\rangle;$$

this subgroup of Sym G is known as the *holomorph* of the group G,

$$\text{Hol}\, G.$$

Let us investigate the structure of the holomorph. If $\alpha \in \text{Aut}\, G$ and $g \in G$, then $\alpha^{-1}g^\rho\alpha$ maps x to $(x^{\alpha^{-1}}g)^\alpha = xg^\alpha$. Consequently $\alpha^{-1}g^\rho\alpha = (g^\alpha)^\rho$, which shows that $G^\rho \lhd \text{Hol}\, G = G^\rho(\text{Aut}\, G)$. Since ρ is regular, $G^\rho \cap \text{Aut}\, G = 1$. Thus the holomorph is a semidirect product.

$$\text{Hol}\, G = (\text{Aut}\, G) \ltimes G^\rho,$$

where an automorphism α of G induces in G^ρ the automorphism $g^\rho \mapsto (g^\alpha)^\rho$. Similarly Hol G is a semidirect product $(\text{Aut}\, G) \ltimes G^\lambda$.

There is a relation between G^λ and G^ρ that involves the concept of a centralizer. If X is a nonempty subset of a group H, the *centralizer* of X in H is defined to be the set of all h in H such that $xh = hx$ for all x in X. We write $C_H(X)$ for this centralizer; it is clearly a subgroup.

1.6.12. *The equations $C_{\text{Hol}\, G}(G^\rho) = G^\lambda$ and $C_{\text{Hol}\, G}(G^\lambda) = G^\rho$ hold for any group G.*

Proof. Evidently $g_1^\rho g_2^\lambda = g_2^\lambda g_1^\rho$ for all $g_i \in G$: for both functions map x to $g_2^{-1}xg_1$. If $\alpha g^\rho \in C_{\text{Hol}\, G}(G^\lambda)$ with $\alpha \in \text{Aut}\, G$, then $\alpha g^\rho x^\lambda = x^\lambda \alpha g^\rho$ for all $x \in G$; this yields $\alpha x^\lambda = x^\lambda \alpha$ since $g^\rho x^\lambda = x^\lambda g^\rho$. Hence $x^\lambda = \alpha^{-1}x^\lambda\alpha = (x^\alpha)^\lambda$ and $x^\alpha = x$ for all x because λ is faithful: thus $\alpha = 1$ and $\alpha g^\rho = g^\rho \in G^\rho$. It follows that $C_{\text{Hol}\, G}(G^\lambda) = G^\rho$. The second statement can be proved in a similar way. □

Conjugacy Classes and Centralizers

Apart from left and right multiplication there is another natural way of representing a group G as a permutation group on its underlying set, as was implied by our discussion of the holomorph, namely by conjugation. If $g \in G$, the function $g^\tau: x \mapsto g^{-1}xg$ is a permutation of G and $\tau: G \to \text{Sym } G$ is a permutation representation. The orbit of x consists of all the conjugates of x, a set which is known as the *conjugacy class of* x. Thus G is partitioned into conjugacy classes. The stabilizer of x is simply the *centralizer*

$$C_G(x) = \{g \in G | gx = xg\}.$$

Hence $|G : C_G(x)|$ = the cardinality of the conjugacy class of x. Also $\{x\}$ is a conjugacy class if and only if x belongs to the center of G.

Class Number and Class Equation

Let G be a finite group. The number h of distinct conjugacy classes of G is known as the *class number* of G. Suppose that the numbers of elements in the conjugacy classes are $n_1, n_2, \ldots, n_h$. Then $n_i = |G : C_G(x_i)|$ where x_i is any element of the ith conjugacy class. These integers satisfy the *class equation*

$$|G| = n_1 + n_2 + \cdots + n_h;$$

they also divide $|G : \zeta G|$ since $\zeta G \leq C_G(x_i)$. The number of n_i which equal 1 is precisely the order of ζG.

Normalizers

If X is a nonempty subset and g is an element of a group G, the *conjugate of X by g* is the subset

$$X^g \equiv g^{-1}Xg = \{g^{-1}xg | x \in X\}.$$

There is a natural action of G on the set of nonempty subsets of G via conjugation. Thus g in G determines the permutation $X \mapsto X^g$. The orbit of X is the set of all conjugates of X in G, while the stabilizer of X is the subgroup

$$N_G(X) = \{g \in G | X^g = X\},$$

which is called the *normalizer* of X in G: the set of conjugates of X in G has cardinality $|G : N_G(X)|$. If $H \leq G$, then $N_G(H)$ is the largest subgroup of G in which H is normal.

1.6.13. *Let H be a subgroup of a group G. Then*

$$C_G(H) \lhd N_G(H)$$

and $N_G(H)/C_G(H)$ is isomorphic with a subgroup of Aut H.

Proof. If $g \in N_G(H)$, let g^τ denote the function $h \mapsto g^{-1}hg$: it is clearly an automorphism of H. What is more, τ: $N_G(H) \to \text{Aut } H$ is a homomorphism whose kernel is exactly $C_G(H)$. The result follows from the First Isomorphism Theorem. □

Applications to Finite Groups—Sylow's Theorem

To convince the reader of their utility we shall use permutation representations to prove some important theorems about finite groups.

If p is a prime, a finite group is called a *p-group* if its order is a power of p. By Lagrange's Theorem the order of each element of a p-group must also be a power of p. The following is the fundamental result about finite p-groups.

1.6.14. *A nontrivial finite p-group has a nontrivial center.*

Proof. Let $p^m = n_1 + \cdots + n_k$ be the class equation of the group; then each n_i divides p^m and hence is a power of p. If the center were trivial, only one n_i would equal 1 and $p^m \equiv 1 \bmod p$, which is impossible since $p^m > 1$. □

1.6.15. *If p is a prime, all groups of order p^2 are abelian.*

Proof. Let $|G| = p^2$ and $C = \zeta G$. Then 1.6.14 shows that $|C| = p$ or p^2 and $|G : C| = p$ or 1. Hence G/C is cyclic, generated by xC, say. Then $G = \langle x, C \rangle$, which implies that G is abelian. □

Sylow Subgroups

Let G be a finite group and p a prime. If $|G| = p^a m$ where $(p, m) = 1$, then a p-subgroup of G cannot have order greater than p^a by Lagrange's Theorem. A p-subgroup of G which has this maximum order p^a is called a *Sylow p-subgroup* of G. We shall prove that Sylow p-subgroups of G always exist and that any two are conjugate—so, in particular, all Sylow p-subgroups of G are isomorphic.

1.6.16 (Sylow's Theorem). *Let G be a finite group and p a prime. Write $|G| = p^a m$ where the integer m is not divisible by p.*

(i) *Every p-subgroup of G is contained in a subgroup of order p^a. In particular, since 1 is a p-subgroup, Sylow p-subgroups always exist.*
(ii) *If n_p is the number of Sylow p-subgroups, $n_p \equiv 1 \bmod p$.*
(iii) *All the Sylow p-subgroups are conjugate in G.*

Proof. Let $\mathscr{S}$ be the set of all *subsets* of G with exactly p^a elements. Then G acts on the set $\mathscr{S}$ by right multiplication, so we have a permutation repre-

sentation of G on $\mathscr{S}$ with degree

$$n = \binom{p^a m}{p^a} = \frac{m(p^a m - 1)\cdots(p^a m - p^a + 1)}{1\cdot 2\cdot \cdots \cdot (p^a - 1)}.$$

Let us show that p does not divide n. Consider the rational number $(p^a m - i)/i$, $1 \leq i < p^a$. If $p^j | i$, then $j < a$ and $p^j | p^a m - i$. On the other hand, if $p^j | p^a m - i$, then $j < a$ and $p^j | i$. Hence $p^a m - i$ and i involve the same power of p, from which it follows that p cannot divide n.

There must therefore exist a G-orbit $\mathscr{S}_1$ such that $|\mathscr{S}_1|$ is not divisible by p. Choose $X \in \mathscr{S}_1$ and put $P = \mathrm{St}_G(X)$. Then $|\mathscr{S}_1| = |G:P|$, whence $p \nmid |G:P|$ and $p^a | |P|$. On the other hand, for a fixed x in X the number of distinct elements xg, $g \in P$, equals $|P|$; therefore $|P| \leq p^a$ and $|P| = p^a$. Thus P is a Sylow p-subgroup of G.

Next let $\mathscr{T}$ denote the set of all conjugates of P in G. Then P acts on $\mathscr{T}$ by means of conjugation. According to 1.6.1 the number of elements in a P-orbit is a power of p. If $\{P_1\}$ is a P-orbit with a single element, then $P_1 \lhd \langle P, P_1 \rangle$ and PP_1 is a subgroup; its order equals $|P|\cdot|P_1|/|P \cap P_1|$, a power of p which cannot exceed $|P| = p^\alpha$. Since $P \leq PP_1$, it follows that $P = PP_1$ and $P = P_1$. Hence $\{P\}$ is the only P-orbit with just one element. Writing n_p for $|\mathscr{T}|$, we conclude that $n_p \equiv 1 \bmod p$.

Finally suppose that P_2 is a p-subgroup of G which is contained in no conjugate of P. Now P_2 too acts on $\mathscr{T}$ by conjugation. If $\{P_3\}$ were a P_2-orbit, it would follow just as above that P_2P_3 is a p-subgroup and $P_2 \leq P_3$; but this contradicts our choice of P_2. Hence every P_2-orbit has more than one element, which implies that $|\mathscr{T}| = n_p \equiv 0 \bmod p$, another contradiction. □

1.6.17 (Cauchy's Theorem). *If a prime p divides the order of a finite group, the group contains an element of order p.*

Cauchy's Theorem is of course a special case of Sylow's Theorem.

Suppose that P is a Sylow p-subgroup of the finite group G. Then the number n_p of Sylow p-subgroups of G is by Sylow's Theorem equal to $|G:N_G(P)|$. So we have the following information about n_p:

$$n_p \,|\, |G:P| \qquad \text{and} \qquad n_p \equiv 1 \mod p.$$

An Illustration

Let us use these facts to prove that *there exist no simple groups of order* 300. Suppose that G is such a group. Since $300 = 2^2 \cdot 3 \cdot 5^2$, a Sylow 5-subgroup of G has order 25. Now $n_5 \equiv 1 \bmod 5$ and n_5 divides $300/25 = 12$; thus $n_5 = 1$ or 6. But $n_5 = 1$ would mean that there was a unique Sylow 5-subgroup which would then have to be normal. Therefore $n_5 = 6$ and G has a

subgroup of index 6. It follows from 1.6.6 that G is isomorphic with a subgroup of S_6, yet 300 does not divide 6!

We shall take note of some useful facts about Sylow subgroups.

1.6.18. *Let P be a Sylow p-subgroup of a finite group G.*

(i) *If $N_G(P) \leq H \leq G$, then $H = N_G(H)$.*
(ii) *If $N \lhd G$, then $P \cap N$ is a Sylow p-subgrup of N and PN/N is a Sylow p-subgroup of G/N.*

Proof. (i) Let $x \in N_G(H)$. Since $P \leq H \lhd N_G(H)$, we have $P^x \leq H$. Obviously P and P^x are Sylow p-subgroups of H, so $P^x = P^h$ for some $h \in H$. Hence $xh^{-1} \in N_G(P) \leq H$ and $x \in H$. It follows that $H = N_G(H)$.

(ii) In the first place $|N : P \cap N| = |PN : P|$, which is prime to p. Since $P \cap N$ is a p-subgroup, it must be a Sylow p-subgroup of N. For PN/N the argument is similar. □

Standard Wreath Products and Sylow Subgroups of the Symmetric Group

If H and K are arbitrary groups, we can think of them as permutation groups on their underlying sets via the right regular representation and form their wreath product $W = H \sim K$: this is called the *standard wreath product*. Its base group is $\mathrm{Dr}_{k \in K} H_k$ where $H_k \simeq H$ and $(H_k)^{k'} = H_{kk'}$. The standard wreath product can be used to describe the Sylow subgroups of the symmetric group S_n.

1.6.19 (Kalužnin)

(i) *A Sylow p-subgroup of S_{p^r} is isomorphic with the standard wreath product $W(p, r) = (\cdots(\mathbb{Z}_p \sim \mathbb{Z}_p) \sim \cdots) \sim \mathbb{Z}_p$, the number of factors being r.*
(ii) *If the positive integer n is written in the form $a_0 + a_1 p + \cdots + a_{i-1} p^{i-1}$ where a_j is integral and $0 \leq a_j < p$, a Sylow p-subgroup of S_n is isomorphic with the direct product of a_1 copies of $W(p, 1)$, a_2 copies of $W(p, 2), \ldots$ and a_{i-1} copies of $W(p, i - 1)$.*

Proof. The order of a Sylow p-subgroup of S_n is the largest power of p dividing $n!$. Now the number of integers among $1, 2, \ldots, n$ divisible by p is $[n/p]$, by p^2 is $[n/p^2]$, etc. Counting the power of p contributed in each case, we find that the order of a Sylow p-subgroup of S_n is p^m where $m = ([n/p] - [n/p^2]) + 2([n/p^2] - [n/p^3]) + \cdots$. Therefore

$$m = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots.$$

When $n = p^r$, this becomes $m = 1 + p + \cdots + p^{r-1}$.

Let us prove that a Sylow p-subgroup of S_{p^r} is of the required type by induction on r, the case $r = 0$ being obvious. Assume that S_{p^r} has a Sylow p-subgroup P of the sort described. Consider the permutation

$$\pi = (1, 1 + p^r, \ldots, 1 + (p-1)p^r)(2, 2 + p^r, \ldots, 2 + (p-1)p^r) \cdots$$
$$(p^r, p^r + p^r, \ldots, p^r + (p-1)p^r):$$

then $\pi \in S_{p^{r+1}}$ and $\pi^p = 1$. Let S_{p^r} be regarded as a subgroup of $S_{p^{r+1}}$ through its action on $\{1, 2, \ldots, p^r\}$, the other symbols being fixed. Then $P_i = \pi^{-i}P\pi^i$ affects only the symbols $j + ip^r$, where $j = 1, 2, \ldots, p^r$. Hence $P = P_0, P_1, \ldots, P_{p-1}$ generate their direct product; also $\pi^{-1}P_i\pi = P_{i+1}$, $0 \leq i < p - 1$, and $\pi^{-1}P_{p-1}\pi = P_0$. Thus $\langle \pi, P \rangle \simeq P \sim \langle \pi \rangle$, the standard wreath product. Since $|P \sim \langle \pi \rangle| = |P|^p \cdot p = p^{mp+1} = p^{1+p+p^2+\cdots+p^r}$, it follows that $\langle \pi, P \rangle$ is a Sylow p-subgroup of $S_{p^{r+1}}$.

In the case of a general S_n we partition the integers $1, \ldots, n$ into a_{i-1} batches of p^{i-1} integers, a_{i-2} batches of $p^{i-2}, \ldots$ and a_0 singletons, using the decomposition $n = a_0 + a_1 p + \cdots + a_{i-1}p^{i-1}$. Take a Sylow p-subgroup of the symmetric group on each batch of p^j elements and regard these as subgroups of S_n in the natural way. These p-subgroups generate their direct product, which therefore has order p^{m_1} where

$$m_1 = a_{i-1}(1 + p + \cdots + p^{i-2}) + a_{i-2}(1 + p + \cdots + p^{i-3}) + \cdots + a_1.$$

But it is easy to show that $m_1 = [n/p] + [n/p^2] + \cdots$. Thus we have constructed a Sylow p-subgroup of S_n. □

Exercises 1.6

1. If H and K are permutation groups on finite sets X and Y, show that the order of $H \quad K$ is $|H|^{|Y|}|K|$.

*2. Let G be a permutation group on a finite set X. If $\pi \in G$, define Fix π to be the set of *fixed points* of π, that is, all x in X such that $x\pi = x$. Prove that the number of G-orbits equals
$$\frac{1}{|G|} \sum_{\pi \in G} |\mathrm{Fix}(\pi)|.$$

3. Prove that a finite transitive permutation group of order > 1 contains an element with no fixed points.

*4. If H and K are finite groups, prove that the class number of $H \times K$ equals the product of the class numbers of H and K.

5. Describe the conjugacy classes of S_n.

6. Find the conjugacy classes of A_5 and deduce that A_5 is a simple group.

7. If p is a prime, a group of order p^2 is isomorphic with $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

8. Let G be a finite group. Prove that elements in the same conjugacy class have conjugate centralizers. If $c_1, c_2, \ldots, c_h$ are the orders of the centralizers of elements from the distinct conjugacy classes, prove that $1/c_1 + 1/c_2 + \cdots + 1/c_h = 1$. Deduce that there exist only finitely many finite groups with given class number h. Find all finite groups with class number 3 or less.

9. Prove that $\mathrm{Hol}\, \mathbb{Z}_3 \simeq S_3$.

10. Let H be a Sylow p-subgroup of a finite group G and let K be a subgroup of G. Is it always true that $H \cap K$ is a Sylow p-subgroup of K?

11. Prove that there are no simple groups of order 312, or 616, or 1960.

*12. Show that the only simple group of order 60 is A_5. [*Hint*: Find a subgroup with index 5.]

*13. If p and q are distinct primes, prove that a group of order pq has a normal Sylow subgroup. If $p \not\equiv 1 \bmod q$ and $q \not\equiv 1 \bmod p$, the group is cyclic.

*14. Let $W = H \wr K$ be the standard wreath product of an abelian group $H \neq 1$ and an arbitrary group K. Prove that the center of W equals the set of elements in the base group all of whose component are equal. (This is called the *diagonal subgroup* of the base group.) Hence $\zeta W = 1$ if K is infinite.

15. Prove that the standard wreath product $\mathbb{Z} \wr \mathbb{Z}$ is finitely generated but has a nonfinitely generated subgroup.

*16. Prove that the standard wreath product $\mathbb{Z}_2 \wr \mathbb{Z}_2$ is isomorphic with D_8.

17. Identify the isomorphism types of the Sylow subgroups of S_6.

*18. Prove that $\mathrm{Aut}\, A_5 \simeq S_5$. [*Hint*: Let P be a Sylow 5-subgroup of A_5 and let α be an automorphism of A_5. Show that $\alpha \equiv \beta \bmod \mathrm{Inn}\, A_5$ for some automorphism β which leaves P invariant.]

19. Let G be a group of order $2m$ where m is odd. Prove that G contains a normal subgroup of order m. [*Hint*: Denote by ρ the regular representation of G: find an odd permutation in G^ρ.]

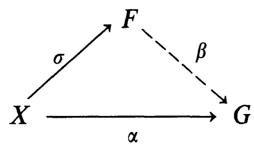
20. Let $G = H \mathrm{wr} K$ where $K \neq 1$. Prove that $B' \leq [B, K]$ where B is the base group. Deduce that $G/[B, K] \simeq (H/H') \times K$.

CHAPTER 2

Free Groups and Presentations

2.1. Free Groups

Let F be a group, X a nonempty set, and $\sigma: X \to F$ a function. Then F, or more exactly (F, σ), is said to be *free* on X if to each function α from X to a group G there corresponds a unique homomorphism $\beta: F \to G$ such that $\alpha = \sigma\beta$: this equation expresses the *commutativity* of the following diagram of sets and functions:



A group which is free on some set is called a *free group*.

The function $\sigma: X \to F$ *is necessarily injective*. For suppose that $x_1\sigma = x_2\sigma$ and $x_1 \neq x_2$: let G be a group with at least two distinct elements g_1 and g_2 and choose a function $\alpha: X \to G$ such that $x_1\alpha = g_1$ and $x_2\alpha = g_2$. Then $x_1\sigma\beta = x_2\sigma\beta$, whence $x_1\alpha = x_2\alpha$ and $g_1 = g_2$, a contradiction. Clearly F is also free on $\operatorname{Im} \sigma$, the inclusion map $\operatorname{Im} \sigma \to F$ taking the place of σ. Hence a free group is always free on a subset: in this case the commutativity of the diagram says that the restriction of β to X is α, so that β is the *unique extension* of α to F.

Another consequence of the definition is that $\operatorname{Im} \sigma$ *generates* F. Since this will follow from our construction of free groups, we need not prove it now.

Constructing Free Groups

There is nothing in the definition to show that free groups actually exist, a deficiency which will now be remedied.

2.1.1. *If X is a nonempty set, there exists a group F and a function $\sigma: X \to F$ such that (F, σ) is free on X and $F = \langle \mathrm{Im}\ \sigma \rangle$.*

Proof. Choose a set disjoint from X with the same cardinality: for notational reasons we shall denote this by $X^{-1} = \{x^{-1} | x \in X\}$ where of course x^{-1} is merely a symbol. By a *word* in X is meant a finite sequence of symbols from $X \cup X^{-1}$, written for convenience in the form

$$w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r},$$

$x_i \in X$, $\varepsilon_i = \pm 1$, $r \geq 0$: in case $r = 0$ the sequence is empty and w is the *empty word*, which will be written 1. Of course two words are to be considered equal if and only if they have the same elements in corresponding positions.

The *product* of two words $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ and $v = y_1^{\eta_1} \cdots y_s^{\eta_s}$ is formed by juxtaposition: thus

$$wv = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} y_1^{\eta_1} \cdots y_s^{\eta_s},$$

with the convention that $w1 = w = 1w$. The *inverse* of w is the word $w^{-1} = x_r^{-\varepsilon_r} \cdots x_1^{-\varepsilon_1}$ and $1^{-1} = 1$.

Let S denote the set of all words in X. We define an equivalence relation on S in the following manner. Two words w and v are said to be *equivalent*, in symbols $w \sim v$, if it is possible to pass from one word to the other by means of a finite sequence of operations of the following types:

(a) insertion of an xx^{-1} or an $x^{-1}x$ $(x \in X)$, as consecutive elements of a word;
(b) deletion of such an xx^{-1} or $x^{-1}x$.

It should be clear to the reader that the relation $\sim$ is an equivalence relation. The equivalence class to which w belongs will be denoted by

$$[w].$$

Define F to be the set of all equivalence classes. We plan to make F into a group. If $w \sim w'$ and $v \sim v'$, one sees at once that $wv \sim w'v'$, so that it is meaningful to define the product of $[w]$ and $[v]$ by means of the equation

$$[w][v] = [wv].$$

Then $[w][1] = [w] = [1][w]$ and $[w][w^{-1}] = [ww^{-1}] = [1]$. Moreover the product is associative: for $(wv)u = w(vu)$ is obviously true and hence $([w][v]) \cdot [u] = [(wv)u] = [w(vu)] = [w] \cdot ([v][u])$. It follows that F is a group with respect to this binary operation: the identity element is $[1]$ and the inverse of $[w]$ is $[w^{-1}]$.

Define a function $\sigma: X \to F$ by the rule $x\sigma = [x]$. We shall prove that (F, σ) is free on X. Suppose that $\alpha: X \to G$ is a function from X to some group G. First we form a function $\bar{\beta}$ from the set of all words in X to G by mapping $x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ to $g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r}$ where $g_i = x_i^{\alpha}$. Now $w \sim v$ implies that $w^{\bar{\beta}} = v^{\bar{\beta}}$ because in the group G products like gg^{-1} or $g^{-1}g$ equal 1_G. It is therefore possible to define a function $\beta: F \to G$ by $[w]^{\beta} = w^{\bar{\beta}}$. Then $([w][v])^{\beta} = [wv]^{\beta} = (wv)^{\bar{\beta}} = w^{\bar{\beta}}v^{\bar{\beta}}$ by definition of $\bar{\beta}$. Hence $([w][v])^{\beta} = [w]^{\beta}[v]^{\beta}$ and β is a homomorphism from F to G. Moreover $x^{\sigma\beta} = [x]^{\beta} = x^{\bar{\beta}} = x^{\alpha}$ for $x \in X$. Finally, if $\gamma: F \to G$ is another homomorphism such that $\sigma\gamma = \alpha$, then $\sigma\gamma = \sigma\beta$ and γ and β agree on Im σ; but clearly $F = \langle \text{Im } \sigma \rangle$, so $\gamma = \beta$. □

Reduced Words

Let us examine the construction just described with a view to obtaining a convenient description of the elements of the free group F.

A word w in X is called *reduced* if it contains no pair of consecutive symbols of the form xx^{-1} or $x^{-1}x$, $(x \in X)$. By convention the empty word is reduced. If w is an arbitrary word, we can delete from w all consecutive pairs xx^{-1} or $x^{-1}x$ to obtain an equivalent word. By repeating this procedure a finite number of times we shall eventually reach a reduced word which is equivalent to w. Thus each equivalence class of words contains a reduced word. The important point to establish is that there is just one reduced word in a class.

2.1.2. *Each equivalence class of words in X contains a unique reduced word.*

Proof. A direct approach to proving uniqueness would involve tedious cancellation arguments. To avoid these we introduce a permutation representation of the free group F on the set of all reduced words R. First of all, let $u \in X \cup X^{-1}$ and define a function $u': R \to R$ by the rule

$$(x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r})u' = \begin{cases} x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}u & \text{if } u \neq x_r^{-\varepsilon_r} \\ x_1^{\varepsilon_1} \cdots x_{r-1}^{\varepsilon_{r-1}} & \text{if } u = x_r^{-\varepsilon_r} \end{cases}$$

where, of course, $x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ is reduced.

Then u' is a permutation of R since $(u^{-1})'$ is obviously its inverse. We use the function from X to Sym(R) in which $x \mapsto x'$, and the defining property of free groups, to produce a homomorphism $\theta: F \to \text{Sym}(R)$ such that $[x]^{\theta} = x'$.

Now let v and w be two equivalent reduced words. Then $[v] = [w]$ and $[v]^{\theta} = [w]^{\theta}$. If $v = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$, then $[v] = [x_1^{\varepsilon_1}] \cdots [x_r^{\varepsilon_r}]$ and $[v]^{\theta} = (x_1^{\varepsilon_1})' \cdots (x_r^{\varepsilon_r})'$. Applying $[v]^{\theta}$ to the empty word, we obtain $x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r} = v$, since this is reduced. Similarly $[w]^{\theta}$ sends the empty word to w. Therefore $v = w$.

Normal Form

By 2.1.2 every element of the constructed free group F can be uniquely written in the form $[w]$ with w a reduced word, say $w = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ where $\varepsilon_i = \pm 1$, $r \geq 0$ and no xx^{-1} or $x^{-1}x$ with $x \in X$ occurs in the word. By definition of multiplication in F we have $[w] = [x_1]^{\varepsilon_1} \cdots [x_r]^{\varepsilon_r}$. Multiplying together consecutive terms involving the same element x_i, we deduce that, after relabeling the x_i's, the element $[w]$ may be written in the form

$$[w] = [x_1]^{l_1} \cdots [x_s]^{l_s}$$

where $s \geq 0$, l_i is a nonzero integer and $x_i \neq x_{i+1}$. Notice that the original reduced word can be reassembled from this, so the expression is unique.

To simplify the notation we shall identify w with $[w]$. By this convention each element of F can be uniquely written in the form

$$w = x_1^{l_1} x_2^{l_2} \cdots x_s^{l_s},$$

where $s \geq 0$, $l_i \neq 0$, and $x_i \neq x_{i+1}$. This is called the *normal form* of w. Sometimes it is convenient to abbreviate it to $w = w(x_1, \ldots, x_s)$ or even to $w = w(x)$.

The existence of a normal form is characteristic of free groups, as the next result shows.

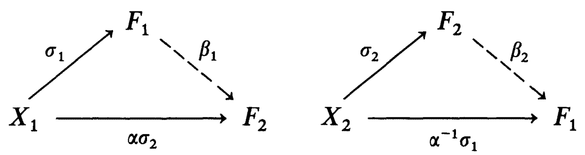
2.1.3. *Let G be a group and X a subset of G. Assume that each element g of G can be uniquely written in the form $g = x_1^{l_1} x_2^{l_2} \cdots x_s^{l_s}$ where $x_i \in X$, $s \geq 0$, $l_i \neq 0$, and $x_i \neq x_{i+1}$. Then G is free on X.*

Proof. Let F be a free group on the set X with associated injection $\sigma: X \to F$. By the mapping property there is a homomorphism $\beta: F \to G$ such that $\sigma\beta: X \to G$ is the inclusion map. Since $G = \langle X \rangle$, we see that β is surjective. It is injective by the uniqueness of the normal form. □

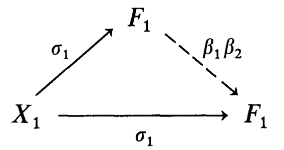
As one might expect, free groups on sets of equal cardinality are isomorphic.

2.1.4. *If F_1 is free on X_1 and F_2 is free on X_2 and if $|X_1| = |X_2|$, then $F_1 \simeq F_2$.*

Proof. Let $\sigma_1: X_1 \to F_1$ and $\sigma_2: X_2 \to F_2$ be the given injections and let $\alpha: X_1 \to X_2$ be a bijection. Then there are commutative diagrams



with β_1 and β_2 homomorphisms. Hence $\sigma_1\beta_1\beta_2 = \alpha\sigma_2\beta_2 = \alpha\alpha^{-1}\sigma_1 = \sigma_1$ and the diagram



commutes. But the identity map 1_{F_1} on F_1 will also make this diagram commute, so $\beta_1\beta_2 = 1_{F_1}$ by uniqueness. A similar argument yields $\beta_2\beta_1 = 1_{F_2}$, so that β_1 is an isomorphism and $F_1 \simeq F_2$. □

Conversely, if $F_1 \simeq F_2$, *then* $|X_1| = |X_2|$ — we shall postpone the proof until 2.3.9 below (see also Exercise 2.1.7). This makes it possible to define the *rank* of a free group as the cardinality of any set on which it is free. Notice that by 2.1.4 a free group on a set X is isomorphic with the free group on X whose elements are the reduced words in X.

The following is a consequence of 2.1.4 and 2.1.1; *if* (F, σ) *is free on a set* X, *then* Im σ *generates* F.

Two Examples of Free Groups

Let us see how free groups occur in nature.

(i) Consider functions α and β on the set $\mathbb{C} \cup \{\infty\}$ defined by the rules

$$(x)\alpha = x + 2 \qquad \text{and} \qquad (x)\beta = \frac{x}{2x + 1}.$$

Here the symbol ∞ is subject to such formal rules as $1/0 = \infty$ and $\infty/\infty = 1$. Then α and β are bijections since they have inverses, namely $(x)\alpha^{-1} = x - 2$ and $(x)\beta^{-1} = x/(1 - 2x)$. Thus α and β generate a group of permutations F of $\mathbb{C} \cup \{\infty\}$; we claim that F is free on the set $\{\alpha, \beta\}$.

To see this observe that a nonzero power of α maps the interior of the unit circle $|z| = 1$ to the exterior and a nonzero power of β maps the exterior of the unit circle to the interior with 0 removed: the second statement is most easily understood from the equation $(1/x)\beta = 1/(x + 2)$. From this it is easy to see that no nontrivial reduced word in $\{\alpha, \beta\}$ can equal 1. Hence every element of F has a unique expression as a reduced word. It now follows from 2.1.3 that F is free on $\{\alpha, \beta\}$.

(ii) Our second example is of a free group generated by matrices. The functions α and β discussed in (i) are instances of the mapping of $\mathbb{C} \cup \{\infty\}$

$$\lambda(a, b, c, d)\colon x \mapsto \frac{ax + b}{cx + d},$$

where $ad - bc \neq 0$ and $a, b, c, d \in \mathbb{C}$. Such a mapping is known as a *linear*

fractional transformation. Now it is easy to show that the function

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \lambda(a, c, b, d)$$

is a homomorphism from $GL(2, \mathbb{C})$ to the group of all linear fractional transformations of $\mathbb{C}$ in which

$$A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

map to α and β respectively. Since no nontrivial reduced word in $\{\alpha, \beta\}$ can equal 1, the same is true of reduced words in $\{A, B\}$. Consequently *the group $\langle A, B\rangle$ is free on $\{A, B\}$.*

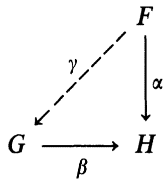
The enormous importance of free groups in group theory is underscored by the following result.

2.1.5. *Let G be a group generated by a subset X and let F be a free group on a set Y. If $\alpha: Y \to X$ is a surjection, it extends to an epimorphism from F to G. In particular every group is an image of a free group.*

Proof. The function α extends to a homomorphism from F to G which is an epimorphism since $G = \langle X\rangle$. □

Finally in this section another useful property of free groups.

2.1.6 (The Projective Property of Free Groups). *Let F be a free group and let G and H be some other groups. Assume that $\alpha: F \to H$ is a homomorphism and $\beta: G \to H$ an epimorphism. Then there is a homomorphism $\gamma: F \to G$ such that $\gamma\beta = \alpha$, that is to say, such that the diagram*



commutes.

Proof. Let F be free on a subset X. If $x \in X$, then $x^\alpha \in H = \text{Im}\,\beta$, so there is a g_x in G such that $g_x^\beta = x^\alpha$. By the defining property of free groups we can extend the function $x \mapsto g_x$ to a homomorphism $\gamma: F \to G$. Since $x^{\gamma\beta} = g_x^\beta = x^\alpha$ for all x in X and X generates F, it follows that $\gamma\beta = \alpha$. □

In fact a group which possesses this projective property is necessarily free (Exercise 6.1.4), so the property characterizes free groups.

EXERCISES 2.1

1. Prove that free groups are torsion-free.
2. Prove that a free group of rank > 1 has trivial center.
3. A free group is abelian if and only if it is infinite cyclic.
4. Let a be a complex number such that $|a| \geq 2$. Prove that $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ generate a free group.

*5. If F is a free group on a subset X and $\varnothing \neq Y \subset X$, prove that F/Y^F is free on $X \backslash Y$.

6. If $N \lhd G$ and G/N is free, prove that there is a subgroup H such that $G = HN$ and $H \cap N = 1$. (Use the projective property.)
7. If F_i is free on X_i, $i = 1, 2$, and $F_1 \simeq F_2$, prove that $|X_1| = |X_2|$ [*Hint*: Consider $\mathrm{Hom}(F_i, \mathbb{Z}_2)$ and view it as a vector space over $\mathbb{Z}_2$.]
8. If (F, σ) is free on a set X, prove *from the definition* that $\mathrm{Im}\,\sigma$ generates F.
9. Let F be a free group on a subset X. If $x \in X$ and $f \in F$, define $\sigma_x(f)$ to be the sum of the exponents of x in the reduced form of f. Prove that $f \in F'$ if and only if $\sigma_x(f) = 0$ for all x in X.
10. Let F be a free group and suppose that H is a subgroup with finite index. Prove that every nontrivial subgroup of F intersects H nontrivially.

2.2. Presentations of Groups

We have seen in 2.1.5 that every group is obtainable as an image of a free group. An actual description of a group as such an image is called a presentation. More exactly a *free presentation* of a group G is an epimorphism π from a free group F to G. Thus if $R = \mathrm{Ker}\,\pi$, we have $R \lhd F$ and $F/R \simeq G$. The elements of R are called the *relators* of the presentation.

For example let F be the free group on a set $Y = \{y_g | 1 \neq g \in G\}$ and let a homomorphism $\pi\colon F \to G$ be defined by $y_g^\pi = g$. Then π is called the *standard presentation* of G.

Suppose that $\pi\colon F \to G$ is a given presentation of a group G. Choose a set of free generators for F, say Y, and a subset S of F such that $S^F = \mathrm{Ker}\,\pi$. If $X = Y^\pi$, then clearly X is a set of generators for G. Next $r \in F$ is a relator of π if and only if it can be written in the form $(s_1^{\varepsilon_1})^{f_1} \cdots (s_k^{\varepsilon_k})^{f_k}$ where $s_i \in S$, $\varepsilon_i = \pm 1$, $f_i \in F$. If this is the case, we sometimes say that r is a *consequence* of S. The presentation π, together with the choice of Y and S, determines *a set of generators and defining relators* for G, in symbols

$$G = \langle Y | S \rangle. \tag{1}$$

In practice it is often more convenient to list the generators of G and the

defining relations $s(x) = 1$, $s \in S$, in these generators X; thus

$$G = \langle X \mid s(x) = 1, s \in S \rangle. \tag{2}$$

We shall sometimes refer to (1) or (2) as a presentation of G.

Conversely it is easy to construct, in principle at least, a group having a presentation with a given set of generators and relators. Let Y be any non-empty set and let S be a subset of the free group on Y. Define R to be the normal closure of S in F and put $G = F/R$. Then the natural homomorphism $\pi: F \to G$ is a presentation of G and G has the set of generators and defining relators $\langle Y \mid S \rangle$.

The following result is frequently useful in the discussion of groups with similar presentations.

2.2.1 (von Dyck's Theorem). *Let G and H be groups with presentations $\varepsilon: F \to G$ and $\delta: F \to H$ such that each relator of ε is also a relator of δ. Then the function $f^\varepsilon \mapsto f^\delta$ is a well-defined epimorphism from G to H.*

Proof. It follows from the hypothesis that $\operatorname{Ker} \varepsilon \leq \operatorname{Ker} \delta$. If $g \in G$, then $g = f^\varepsilon$ for some $f \in F$: moreover f^δ is uniquely determined by g since if $g = f_1^\varepsilon$, then $f = f_1 k$ where $k \in \operatorname{Ker} \varepsilon \leq \operatorname{Ker} \delta$, and $f^\delta = f_1^\delta$. Obviously $f^\varepsilon \mapsto f^\delta$ is an epimorphism. □

Examples of Presentations

In practice it is usually difficult to obtain information about a group from a given presentation: in fact there is no general procedure for deciding if the group has order 1. Success usually depends upon finding a model which realizes the presentation. Some examples will illustrate the point.

(I) $G = \langle x, y \mid x^2 = 1, y^2 = 1 \rangle$. This group is called the *infinite dihedral group* D_∞. Set $a = xy$; then $G = \langle x, a \rangle$ and $x^{-1}ax = yx = a^{-1}$. Conversely the original relations $x^2 = 1 = y^2$ are consequences of the relations $x^2 = 1$ and $x^{-1}ax = a^{-1}$ (strictly $x^{-1}axa = 1$): for given the latter one has $y^2 = (x^{-1}a)^2 = x^{-1}axa = 1$. Thus G also has the presentation

$$\langle x, a \mid x^2 = 1, x^{-1}ax = a^{-1} \rangle.$$

This group may be realized as a semidirect product $\bar{G} = X \ltimes A$ where $A = \langle \bar{a} \rangle$ is infinite cyclic, $X = \langle \bar{x} \rangle$ is cyclic of order 2 and $\bar{x}$ conjugates an element of A into its inverse. For by von Dyck's Theorem there is an epimorphism $\theta: G \to \bar{G}$ in which $x \mapsto \bar{x}$ and $a \mapsto \bar{a}$. A typical element of G has the form $x^r a^s$, $r = 0, 1$, since $\langle a \rangle \lhd G$: this maps under θ to $\bar{x}^r \bar{a}^s$, which is trivial only if $r = 0 = s$. Thus $G \simeq \bar{G}$.

(II) $G = \langle x, y \mid x^2 = y^2 = (xy)^n = 1 \rangle$, where $n \geq 2$. This is the dihedral group D_{2n} of order $2n$. Writing $a = xy$ we see that

$$\langle x, a \mid x^2 = a^n = 1, x^{-1}ax = a^{-1} \rangle$$

is another presentation of G. As above G is isomorphic with the semidirect product $X \ltimes A$ where A is cyclic of order n, X is cyclic of order 2 and the generator of X conjugates elements of A into their inverses.

(III) *A presentation of the symmetric group*

2.2.2. *If $n > 1$, there is a presentation of the symmetric group S_n with generators $x_1, x_2, \dots, x_{n-1}$ and relations*

$$1 = x_i^2 = (x_j x_{j+1})^3 = (x_k x_l)^2,$$

where $1 \leq i \leq n-1$, $1 \leq j \leq n-2$, and $1 \leq l < k-1 < n-1$.

Proof. Let G be a group with the generators and defining relations listed. We shall prove first that $|G| \leq n!$. If $H = \langle x_1, \dots, x_{n-2} \rangle$, it follows from von Dyck's Theorem and an induction on n that $|H| \leq (n-1)!$. Therefore it will be enough to show that $|G:H| \leq n$.

Consider the n right cosets $H, Hx_{n-1}, Hx_{n-1}x_{n-2}, \dots, Hx_{n-1}x_{n-2}\cdots x_1$. Let us prove that right multiplication by any x_j permutes these cosets. If $j < i-1$, then $x_i x_j = (x_i x_j)^{-1} = x_j x_i$ by the defining relations: hence $(Hx_{n-1}\cdots x_i)x_j = Hx_j x_{n-1}\cdots x_i = Hx_{n-1}\cdots x_i$ since $x_j \in H$. Let $j > i$. Since $x_k x_j = x_j x_k$ if $|j-k| > 1$, we have

$$(Hx_{n-1}\cdots x_i)x_j = Hx_{n-1}\cdots x_{j+1}(x_j x_{j-1} x_j)x_{j-2}\cdots x_i:$$

now $(x_{j-1}x_j)^3 = 1$, which implies that $x_{j-1}x_j x_{j-1} = x_j x_{j-1} x_j$. Hence we obtain

$$(Hx_{n-1}\cdots x_i)x_j = Hx_{n-1}\cdots x_{j+1}(x_{j-1}x_j x_{j-1})x_{j-2}\cdots x_i$$

$$= Hx_{j-1}x_{n-1}\cdots x_i = Hx_{n-1}\cdots x_i.$$

Finally

$$(Hx_{n-1}\cdots x_i)x_i = Hx_{n-1}\cdots x_{i+1}$$

and

$$(Hx_{n-1}\cdots x_i)x_{i-1} = Hx_{n-1}\cdots x_i x_{i-1},$$

as required. Since the x_j generate G, every element of G lies in one of these cosets and $|G:H| \leq n$.

To complete the proof we show that S_n realizes the presentation. To this end consider the $n-1$ *adjacent* transpositions $\pi_i = (i, i+1)$, $i = 1, \dots, n-1$. Every permutation is a product of transpositions and every transposition is a product of adjacent transpositions—as is readily seen by repeated use of the formula $(i, j) = (j-1, j)(i, j-1)(j-1, j)$, $i < j-1$. Hence $S_n = \langle \pi_1, \dots, \pi_{n-1} \rangle$. It is easy to verify that $1 = \pi_i^2 = (\pi_j \pi_{j+1})^3 = (\pi_k \pi_l)^2$ if $1 \leq i \leq n-1$, $1 \leq j \leq n-2$, and $l < k-1 < n-1$. By 2.2.1 there is an epimorphism $\alpha: G \to S_n$ in which $x_i \mapsto \pi_i$. Since $|G : \operatorname{Ker} \alpha| = n!$ and $|G| \leq n!$, it follows that $\operatorname{Ker} \alpha = 1$ and α is an isomorphism.

Finitely Presented Groups

A group is said to be *finitely presented* if it has a *finite presentation* $\langle X|R\rangle$, that is, one in which X and R are finite. In other words the group can be specified by a finite set of generators and a finite set of relations. This definition is independent of the particular presentation chosen in the sense of the following result.

2.2.3 (B.H. Neumann). *If X is any set of generators of a finitely presented group G, the group has a finite presentation of the form $\langle X_0|r_1 = r_2 = \cdots = r_t = 1\rangle$ where $X_0 \subseteq X$.*

Proof. Let $G = \langle y_1, \dots, y_m | s_1 = \cdots = s_l = 1\rangle$ be a finite presentation of G. Since $G = \langle X\rangle$, it follows that $G = \langle X_0\rangle$ where $X_0 = \{x_1, \dots, x_n\}$ is a finite subset of X. There are, therefore, expressions for the y_i in terms of the x_j and the x_j in terms of the y_i, say $y_i = w_i(x)$ and $x_j = v_j(y)$. Hence the following relations in the x_j's are valid:

$$s_k(w_1(x), \dots, w_m(x)) = 1, \qquad x_j = v_j(w_1(x), \dots, w_m(x)),$$

$k = 1, \dots, l, j = 1, \dots, n$; there are of course only finitely many of these.

Now let $\bar{G}$ be a group with generators $\bar{x}_1, \dots, \bar{x}_n$ and the above defining relations in $\bar{x}_1, \dots, \bar{x}_n$. By 2.2.1 there is an epimorphism from $\bar{G}$ to G in which $\bar{x}_i \mapsto x_i$. Define $\bar{y}_i = w_i(\bar{x})$; the second set of defining relations shows that $\bar{G} = \langle \bar{y}_1, \dots, \bar{y}_m\rangle$. Since $s_k(\bar{y}) = 1$, there is, by 2.2.1 again, an epimorphism from G to $\bar{G}$ in which $y_i \mapsto \bar{y}_i$. These epimorphisms are mutually inverse, so they are isomorphisms. Hence G is generated by $x_1, \dots, x_n$ subject only to the defining relations in the x_i listed above. □

Examples of finitely presented groups include *cyclic groups*, *free groups of finite rank* (which have no relations), and *finite groups*. To prove the last statement let $\pi: F \to G$ be any presentation of a finite group G such that F is finitely generated; let $R = \operatorname{Ker} \pi$. Then R is finitely generated by 1.6.11. Therefore π is a finite presentation of G. On the other hand, not every finitely generated group is finitely presented, an example being the standard wreath product of two infinite cyclic groups (see 14.1.4).

Further examples of finitely presented groups may be obtained from the next result.

2.2.4 (P. Hall). *Let $N \lhd G$ and suppose that N and G/N are finitely presented groups. Then G is finitely presented.*

Proof. Let N have generators $x_1, \dots, x_m$ and relations $r_1 = \cdots = r_k = 1$, and let G/N have generators $y_1N, \dots, y_nN$ and relations $s_1 = \cdots = s_l = 1_{G/N}$. Obviously G can be generated by $x_1, \dots, x_m, y_1, \dots, y_n$: moreover there are

relations in these generators of the following types:

$$r_i(x) = 1, \qquad s_j(y) = t_j(x) \qquad (i = 1, \dots, k, j = 1, \dots, l),$$
$$y_j^{-1}x_iy_j = u_{ij}(x), \qquad y_jx_iy_j^{-1} = v_{ij}(x) \qquad (i = 1, \dots, m, j = 1, \dots, n).$$

The last two sets of relations express the normality of N in G.

Let $\bar{G}$ be a group with generators $\bar{x}_1, \dots, \bar{x}_m, \bar{y}_1, \dots, \bar{y}_n$ and the above defining relations in the $\bar{x}_i$ and $\bar{y}_j$. By 2.2.1 there is an epimorphism $\alpha: \bar{G} \to G$ such that $\bar{x}_i^\alpha = x_i$ and $\bar{y}_j^\alpha = y_j$: let $K = \operatorname{Ker} \alpha$. Now the restriction of α to $\bar{N} \equiv \langle \bar{x}_1, \dots, \bar{x}_m \rangle$ must be an isomorphism since all relations in the x_i are consequences of the $r_j(x) = 1$: hence $K \cap \bar{N} = 1$. Next $\bar{N} \lhd \bar{G}$ since $\bar{y}_j^{-1}\bar{x}_i\bar{y}_j$ and $\bar{y}_j\bar{x}_i\bar{y}_j^{-1}$ belong to $\bar{N}$. Now α induces an epimorphism from $\bar{G}/\bar{N}$ to G/N in which $\bar{y}_i\bar{N} \mapsto y_iN$: this must be an isomorphism because all relations in the y_iN are consequences of the $s_j(yN) = 1_{G/N}$. Hence $K = 1$ and $\bar{G} \simeq G$, so G is finitely presented. □

For example, if a group G has a chain of subgroups $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_i \lhd G_{i+1} \lhd \cdots \lhd G_n = G$ in which each G_{i+1}/G_i is cyclic, then G is finitely presented. Such groups are called *polycyclic*: they are studied in Chapters 5 and 15.

The Word Problem

Suppose that G is a finitely presented group with generators $x_1, \dots, x_n$ and relators $r_1, \dots, r_k$. Here the r_i are assumed to be explicitly given words in the x_i. The *word problem* is said to be soluble for the presentation if there is an algorithm which, when a word w in the x_i is given, decides whether or not w is a relator, i.e., whether $w = 1$ in G. Roughly speaking, this means that it is possible to decide, at least in principle, whether $w = 1$ in G by machine computation. It is not difficult to see that the question is independent of the particular finite presentation and so it is a question about the group G. We say that G has *soluble word problem* if the word problem is soluble for some—and hence any—finite presentation of G.

A natural approach to the problem is to enumerate the relators of G by listing all consequences of the defining relators $r_1, \dots, r_k$, i.e., all words $(r_{i_1}^{\pm 1})^{f_1} \cdots (r_{i_j}^{\pm 1})^{f_j}$, $(f_i \in F)$. Thus, if w is a relator, it will appear on our list and, given enough time, we will detect it. The difficulty is that if w is not a relator, it will never appear in the course of our enumeration, but this cannot be established in any finite time. What one needs is a way of enumerating the words that are *not* relators. Now it is known that there are sets which are *recursively enumerable* (i.e., capable of machine enumeration), but whose complements are not recursively enumerable. In view of this it is not too surprising that there exist finitely presented groups which have insoluble word problem. This is the famous Boone–Novikov Theorem; for a very readable account see [b57].

Despite this negative result there are significant classes of finitely presented groups for which the word problem is soluble. Here we shall prove just one result. But first a definition. A group G is said to be *residually finite* if, given $g \neq 1$ in G, there is an $N \lhd G$ such that $g \notin N$ and G/N is the finite. (For more on residual properties, see 2.3.)

2.2.5. *Let G be a finitely presented residually finite group. Then G has soluble word problem.*

Proof. We assume that G is given by an explicit finite presentation. Let w be a given word in the generators. We shall describe two procedures to be set in motion, and then explain how they will tell us whether or not $w = 1$ in G. The first procedure simply enumerates all consequences of the defining relators and looks for the word w. If w turns up, then $w = 1$ in G, and the procedure stops.

The second procedure enumerates all finite groups, say by constructing their multiplication tables. For each finite group F, it constructs the (finitely many) homomorphisms θ from G to F; to do this one has to assign an element of F to each generator of G and then check that each defining relator equals 1 in F. For each such homomorphism θ the procecdure then computes w^θ in F, and checks to see if it equals the identity. If ever $w^\theta \neq 1$ in F, then $w \neq 1$ in G, and the procedure stops.

The point is that residual finiteness guarantees that one procedure will stop. Indeed, if $w \neq 1$ in G, then $w \notin N$ for some $N \lhd G$ with $F = G/N$ finite. Thus $w \neq 1$ in F. If the first procedure stops, then $w = 1$ in G; if the second one stops, then $w \neq 1$ in G.

For example, polycyclic groups are finitely presented by 2.2.4, and it is shown in 5.4.17 that they are residually finite. Hence the word problem is soluble for polycyclic groups. The word problem is one of three important decision problems in group theory which were first formulated in 1911 by M. Dehn; the others are the *conjugacy problem*, which asks if there is an algorithm to decide if two elements of a finitely presented group are conjugate, and the *isomorphism problem*: Is there an algorithm to decide whether two given finitely presented groups are isomorphic? All three problems have negative answers in general. For more information on the decision problems of group theory, see [b43] or [b46]. □

Exercises 2.2

1. Show that S_3 has the presentation $\langle x, y \mid x^2 = y^3 = (xy)^2 = 1\rangle$.
2. Show that A_4 has the presentation $\langle x, y \mid x^2 = y^3 = (xy)^3 = 1\rangle$ [*Hint*: Examine the right action of the group on the set of cosets $\langle y\rangle$, $\langle y\rangle x$, $\langle y\rangle xy$, $\langle y\rangle xy^2$.]
3. Show that S_4 has the presentation $\langle x, y \mid x^4 = y^2 = (xy)^3 = 1\rangle$.

4. Let $G = \langle x, y | x^3 = y^3 = (xy)^3 = 1 \rangle$. Prove that $G \simeq \langle t \rangle \ltimes A$ where $t^3 = 1$ and $A = \langle a \rangle \times \langle b \rangle$ is the direct product of two infinite cyclic groups, the action of t being $a^t = b$, $b^t = a^{-1}b^{-1}$. [*Hint*: Prove that $\langle xyx, x^2y \rangle$ is a normal abelian subgroup.]

5. Let p be a prime. Prove that the group $\langle x, y | x^p = y^p = (xy)^p = 1 \rangle$ is infinite if $p > 2$, but that if $p = 2$, it is a Klein 4-group.

6. Let A be an abelian group with generators $x_1, x_2, \ldots, x_n$ and defining relations consisting of $[x_i, x_j] = 1$, $i < j = 1, 2, \ldots, n$, and r further relations. If $r < n$, prove that A is infinite.

7. Suppose that G is a group with n generators and r relations whether $r < n$. Prove that G is infinite.

8. Let G be a finitely presented group and let N be a normal subgroup which is finitely generated as a G-operator group. Prove that G/N is finitely presented.

*9. Let $\pi: F \to G$ be a presentation of a group G and let $R = \text{Ker } \pi$. If A is the subgroup of all automorphisms α of F such that $R^\alpha = R$, show that there is a canonical homomorphism $A \to \text{Aut } G$. Use this to construct an outer automorphism of A_4 (see Exercise 2.2.2).

10. Prove that the group G with generators x, y, z and relations $z^y = z^2$, $x^z = x^2$, $y^x = y^2$ has order 1.

2.3. Varieties of Groups

In this section we shall consider classes of groups which are defined by sets of equations.

Verbal and Marginal Subgroups

Let F be a free group on a countably infinite set $\{x_1, x_2, \ldots\}$ and let W be a nonempty subset of F. If $w = x_{i_1}^{l_1} \cdots x_{i_r}^{l_r} \in W$ and $g_1, \ldots, g_r$ are elements of a group G, we define the *value* of the word w at $(g_1, \ldots, g_r)$ to be $w(g_1, \ldots, g_r) = g_1^{l_1} \cdots g_r^{l_r}$. The subgroup of G generated by all values in G of words in W is called the *verbal subgroup* of G determined by W,

$$W(G) = \langle w(g_1, g_2, \ldots) | g_i \in G, w \in W \rangle.$$

For example, if $W = \{[x_1, x_2]\}$, then $W(G) = G'$, the derived subgroup of G: if $W = \{x_1^n\}$, then $W(G) = G^n$, the subgroup generated by all the nth powers in G.

If $\alpha: G \to H$ is a homomorphism, then $(w(g_1, \ldots, g_r))^\alpha = w(g_1^\alpha, \ldots, g_r^\alpha)$, which shows at once that $(W(G))^\alpha \leq W(H)$. In particular *every verbal subgroup is fully-invariant*. The converse is false in general (Exercise 2.3.3), but it does hold for free groups.

2.3.1 (B.H. Neumann). *A fully-invariant subgroup of a free group is verbal.*

Proof. Let F be free on a set X and let W be a fully-invariant subgroup of F. If $w = w(x_1, \ldots, x_r) \in W$ with $x_i \in X$, choose any r elements $f_1, \ldots, f_r$ of F. Now there is an endomorphism α of F such that $x_i^\alpha = f_i$: hence W contains $w^\alpha = w(f_1, \ldots, f_r)$. So W contains all values of w in F and hence $W = W(F)$. □

If W is a set of words in $x_1, x_2, \ldots$ and G is any group, a normal subgroup N is said to be *W-marginal* in G if

$$w(g_1, \ldots, g_{i-1}, g_i a, g_{i+1}, \ldots, g_r) = w(g_1, \ldots, g_{i-1}, g_i, g_{i+1}, \ldots, g_r)$$

for all $g_i \in G$, $a \in N$ and all $w(x_1, x_2, \ldots, x_r)$ in W. This is equivalent to the requirement: $g_i \equiv h_i \bmod N$, $(1 \leq i \leq r)$, always implies that $w(g_1, \ldots, g_r) = w(h_1, \ldots, h_r)$.

We see from the definition that the W-marginal subgroups of G generate a normal subgroup which is also W-marginal. This is called *the W-marginal subgroup of* G and is written

$$W^*(G).$$

For example, suppose that $W = \{[x_1, x_2]\}$: if $a \in W^*(G)$ and $g \in G$, then $[g, a] = [g, 1a] = [g, 1] = 1$ for all $g \in G$, that is, a belongs to the center of G. Conversely, if $a \in \zeta G$, then $[g_1, g_2 a] = [g_1, g_2]$, so that $W^*(G) = \zeta G$ in this case.

A marginal subgroup is always characteristic but need not be fully-invariant, as the example of the centre shows (Exercise 1.5.9).

The following lemma indicates a connection between verbal and marginal subgroups.

2.3.2. *Let W be a nonempty set of words in $x_1, x_2, \ldots$ and let G be any group. Then $W(G) = 1$ if and only if $W^*(G) = G$.*

Proof. Obviously $W(G) = 1$ implies that $W^*(G) = G$. Suppose that $W^*(G) = G$ and let $g_i \in G$; then $g_i \equiv 1 \bmod G$, whence $w(g_1, \ldots, g_r) = w(1, \ldots, 1) = 1$ and $W(G) = 1$. □

Group-Theoretical Classes and Properties

A *group-theoretical class* (or *class of groups*) $\mathfrak{X}$ is a class—not a set—whose members are groups and which enjoys the following properties: (i) $\mathfrak{X}$ contains a group of order 1; and (ii) $G_1 \simeq G \in \mathfrak{X}$ always implies that $G_1 \in \mathfrak{X}$. For example all finite groups and all abelian groups form classes of groups. More generally, let $\mathscr{P}$ be any *group-theoretical property*, that is, a property pertaining to groups such that a group of order 1 has $\mathscr{P}$, and $G_1 \simeq G$ and G

has $\mathscr{P}$ always imply that G_1 has $\mathscr{P}$. Then the class $\mathfrak{X}^{\mathscr{P}}$ of all groups with $\mathscr{P}$ is clearly a group-theoretical class: likewise to belong to a given group-theoretical class $\mathfrak{X}$ is a group-theoretical property $\mathscr{P}_{\mathfrak{X}}$. Moreover the functions $\mathscr{P} \mapsto \mathfrak{X}^{\mathscr{P}}$ and $\mathfrak{X} \mapsto \mathscr{P}_{\mathfrak{X}}$ are evidently mutually inverse bijections.

For this reason it is often convenient not to distinguish between a group-theoretical property and the class of groups that possess it. A group in a class $\mathfrak{X}$ is called an *$\mathfrak{X}$-group*.

Varieties

A variety is an equationally defined class of groups. More precisely, if W is a set of words in $x_1, x_2, \ldots$, the class of all groups G such that $W(G) = 1$, or equivalently $W^*(G) = G$, is called the *variety* $\mathfrak{B}(W)$ determined by W. We also say that W is a *set of laws* for the variety $\mathfrak{B}(W)$.

Examples

(1) If $W = \{[x_1, x_2]\}$, then $\mathfrak{B}(W)$ is the class of *abelian groups*.

(2) If $W = \{[x_1, x_2], x_1^p\}$ where p is a prime, then $\mathfrak{B}(W)$ is the class of abelian groups of exponent 1 or p, that is, *elementary abelian p-groups*. These are precisely the direct products of groups of order p (see Exercise 1.4.8).

(3) If $W = \{x_1^n\}$, then $\mathfrak{B}(W)$ is the class of groups of exponent dividing n, the so-called *Burnside variety of exponent n*.

(4) Less interesting examples of varieties are the class of groups of order 1 (take $W = \{x_1\}$) and the class of all groups (take $W = \{1\}$).

Residual Classes and Subcartesian Products

Let $\mathfrak{X}$ be a class of groups: a group G is said to be a *residually $\mathfrak{X}$-group* if, given $1 \neq g \in G$, there exists a normal subgroup N_g such that $g \notin N_g$ and $G/N_g \in \mathfrak{X}$. Under these circumstances $\bigcap_{1 \neq g \in G} N_g = 1$. Now consider the function $\iota\colon G \to C = \mathrm{Cr}_{1 \neq g \in G}(G/N_g)$ defined by the rule $(x^\iota)_g = xN_g$. Then it should be clear to the reader that ι is a monomorphism. Notice also that each element of G/N_g occurs as the g-component of some element of $\mathrm{Im}\ \iota$.

We may generalize this situation in the following manner. Let $\{G_\lambda \mid \lambda \in \Lambda\}$ be a family of groups. A group G is said to be a *subcartesian product* of the G_λ if there exists a monomorphism

$$\iota\colon G \to \mathop{\mathrm{Cr}}_{\lambda \in \Lambda} G_\lambda$$

such that for each λ in Λ every element of G_λ occurs as the λ-component of some element of $\mathrm{Im}\ \iota$.

2.3.3. *A group G is a residually $\mathfrak{X}$-group if and only if it is a subcartesian product of $\mathfrak{X}$-groups.*

Proof. We have already proved the necessity. Let G be a subcartesian product of $\mathfrak{X}$-groups G_λ, $\lambda \in \Lambda$, via a monomorphism $\iota: G \to C = \mathrm{Cr}_{\lambda \in \Lambda} G_\lambda$. Define ι_λ to be the composite of ι with the homomorphism $C \to G_\lambda$ that maps each element of C to its λ-component. Let $K_\lambda = \mathrm{Ker}\ \iota_\lambda$. Since ι is injective, $\bigcap_{\lambda \in \Lambda} K_\lambda = 1$. Also $\mathrm{Im}\ \iota_\lambda = G_\lambda$ by the subcartesian property, whence $G/K_\lambda \simeq G_\lambda \in \mathfrak{X}$. If $1 \neq g \in G$, then $g \notin K_\lambda$ for some λ and therefore G is a residually $\mathfrak{X}$-group. □

We wish to apply these ideas to the question: how can one decide whether a given class of groups is a variety? First we observe that there are certain "closure properties" which every variety has: then we show that these properties characterize varieties.

2.3.4. *Every variety is closed with respect to forming subgroups, images, and subcartesian products of its members.*

This is a trivial consequence of the definition of a variety. Much less obvious is the following remarkable result.

2.3.5 (Birkhoff, Kogalovskiĭ, Šain). *A class of groups which is closed with respect to forming homomorphic images and subcartesian products of its members is a variety.*

Proof. Let $\mathfrak{X}$ be such a class of groups and denote by $\mathfrak{B}$ the variety which has as a set of laws all words that are identically equal to 1 in every $\mathfrak{X}$-group. Certainly $\mathfrak{X} \subseteq \mathfrak{B}$: our task is to prove that $\mathfrak{B} \subseteq \mathfrak{X}$. We can certainly assume that $\mathfrak{X}$ contains a group of order > 1 since otherwise $\mathfrak{B} = \mathfrak{X} =$ the class of groups of order 1.

If w is a word (in $x_1, x_2, \ldots$) which is not a law of $\mathfrak{B}$, there is an $\mathfrak{X}$-group $H(w)$ such that w is not identically equal to 1 in $H(w)$. Let $1 \neq G \in \mathfrak{B}$ and choose an infinite set Y whose cardinality is not less than that of G and of each of the $H(w)$'s—keep is mind that there are only countably many words w. Let F be a free group on Y. By choice of Y there is an epimorphism from F to G, say with kernel N: thus $G \simeq F/N$. Let $w \in F \backslash N$ and suppose that $w = w(y_1, \ldots, y_r)$ where $y_i \in Y$. Now $w(x_1, \ldots, x_r)$ is not identically equal to 1 on G, so there is a corresponding $\mathfrak{X}$-group $H(w)$: since w is not identically equal to 1 in $H(w)$, we have $w(h_1, \ldots, h_r) \neq 1$ for some $h_i \in H(w)$. By choice of Y again there is an epimorphism from F to $H(w)$ such that $y_i \mapsto h_i$, $i = 1, \ldots, r$. If K_w is the kernel, then $F/K_w \simeq H(w) \in \mathfrak{X}$. Now let $K = \bigcap_{w \in F \backslash N} K_w$: since $w \notin K_w$, it follows that $K \leq N$. But F/K is a residually $\mathfrak{X}$-group, so $F/K \in \mathfrak{X}$ by 2.3.4. Since $G \simeq F/N$ is an image of F/K, it follows that $G \in \mathfrak{X}$ as required. □

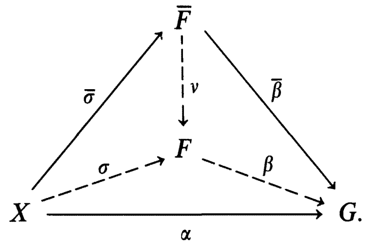
Free $\mathfrak{B}$-Groups

Let $\mathfrak{B}$ be a variety, F a group in $\mathfrak{B}$, X a nonempty set, and $\sigma: X \to F$ a function. Then (F, σ), or simply F, is *$\mathfrak{B}$-free on X* if for each function α from X to a $\mathfrak{B}$-group G there exists a unique homomorphism $\beta: F \to G$ such that $\sigma\beta = \alpha$. When $\mathfrak{B}$ is the variety of all groups, this is just the definition of a free group on X. A group which is $\mathfrak{B}$-free on some set is called a *free $\mathfrak{B}$-group*. Groups which are free in some variety are often said to be *relatively free*.

Free $\mathfrak{B}$-groups are easily described in terms of free groups.

2.3.6. *Let X be a nonempty set, $\bar{F}$ a free group on X, and $\mathfrak{B}$ a variety with a set of laws W. Then $F = \bar{F}/W(\bar{F})$ is a $\mathfrak{B}$-free group on X. Moreover every group which is $\mathfrak{B}$-free on X is isomorphic with F.*

Proof. Let $\bar{\sigma}: X \to \bar{F}$ be the injection associated with the free group $\bar{F}$ and let $\nu: \bar{F} \to F = \bar{F}/W(\bar{F})$ be the natural homomorphism. Put $\sigma = \bar{\sigma}\nu$. Suppose that G is a group in the variety $\mathfrak{B}$ and let $\alpha: X \to G$ be any function. Since $\bar{F}$ is free on X, there exists a unique homomorphism $\bar{\beta}: \bar{F} \to G$ such that $\bar{\sigma}\bar{\beta} = \alpha$. Because $G \in \mathfrak{B}$, we have $W(G) = 1$, so that $W(\bar{F})^{\bar{\beta}} = 1$. Consequently the mapping $xW(\bar{F}) \mapsto x^{\bar{\beta}}$ is a well-defined homomorphism β from F to G. Now $x^{\nu\beta} = (xW(\bar{F}))^{\beta} = x^{\bar{\beta}}$, so $\nu\beta = \bar{\beta}$ and $\sigma\beta = \bar{\sigma}\nu\beta = \bar{\sigma}\bar{\beta} = \alpha$. Hence in the tetrahedral diagram which follows the lower face commutes:



If $\beta': F \to G$ is another such homomorphism, $\bar{\sigma}(\nu\beta') = \sigma\beta' = \alpha = \bar{\sigma}\bar{\beta}$, whence $\nu\beta' = \bar{\beta} = \nu\beta$ by uniqueness of $\bar{\beta}$. Since ν is surjective, $\beta' = \beta$. Hence F is $\mathfrak{B}$-free on X. Just as in 2.1.4 we can prove that $\mathfrak{B}$-free groups on sets of equal cardinality are isomorphic. Hence the result follows. □

If F is $\mathfrak{B}$-free on X, the associated function $\sigma: X \to F$ is a monomorphism, so one may assume that X is a subset of F and that the unique homomorphism β in the definition is an extension of $\alpha: X \to G$ to F.

2.3.7. *Let $\mathfrak{B}$ be a variety and let $G \in \mathfrak{B}$. If G is generated by X, the group F is $\mathfrak{B}$-free on Y and $\alpha: Y \to X$ is a surjection, then α extends to an epimorphism from F to G. In particular every $\mathfrak{B}$-group is an image of a free $\mathfrak{B}$-group.*

Proof. The surjection α extends to a homomorphism from F by definition. Since $G = \langle X \rangle$, this is an epimorphism. □

Free Abelian Groups

A *free abelian group* is a group that is free in the variety of abelian groups. These are of great importance; for example every abelian group is an image of a free abelian group. Also if $\bar{F}$ is a free group on a set X, then $\bar{F}_{ab} = \bar{F}/\bar{F}'$ is free abelian on X. Moreover every free abelian group on X is isomorphic with $\bar{F}_{ab}$; this is by 2.3.6.

It is easy to describe free abelian groups in terms of direct products.

2.3.8.

(i) *If F is a free abelian group on a subset X, then F is the direct product of the infinite cyclic subgroups $\langle x \rangle$, $x \in X$.*
(ii) *Conversely a direct product* $\mathrm{Dr}_{x \in X} C_x$ *in which each C_x is infinite cyclic is free abelian on X.*

Proof. (i) We may assume that $F = \bar{F}_{ab}$ where $\bar{F}$ is free on X. Suppose that $x_{i_1}^{l_1} \cdots x_{i_r}^{l_r} \in \bar{F}'$ where $i_1 < \cdots < i_r$ and $x_j \in X$. Now the sum of the exponents of x_j in any element of $\bar{F}'$ is clearly 0; hence $l_j = 0$. This shows that $\langle x\bar{F}' \rangle$ is infinite cyclic: it also shows that each element of F has a unique expression of the form $x_{i_1}^{l_1} \cdots x_{i_r}^{l_r}\bar{F}'$ where $i_1 < \cdots < i_r$ and $x_j \in X$. By 1.4.8 the group F is the direct product of the $\langle x\bar{F}' \rangle$, $x \in X$.

(ii) Let $D = \mathrm{Dr}_{x \in X} C_x$ and write $C_x = \langle c_x \rangle$. Let $\bar{F}$ be a free group on X: we assume for convenience that $X \subseteq \bar{F}$. There is an epimorphism $\beta: \bar{F} \to D$ in which x is mapped to c_x. Suppose that $y \in \operatorname{Ker} \beta$. Now we can write $y = x_{i_1}^{l_1} \cdots x_{i_r}^{l_r} z$ where $i_1 < \cdots < i_r$, $x_j \in X$ and $z \in \bar{F}'$. But $z^\beta = 1$ since D is abelian. Thus $c_1^{l_1} \cdots c_r^{l_r} = 1$ where $c_j = c_{x_j}$. But this implies that $l_j = 0$ for all j. Hence $\operatorname{Ker} \beta = \bar{F}'$ and $D \simeq \bar{F}_{ab}$. The latter is free abelian on X, so the proof is complete. □

Therefore, if $\bar{F}$ is a free group, $\bar{F}/\bar{F}'$ is a direct product of infinite cyclic groups.

2.3.9. *Let F_1 and F_2 be free abelian groups on sets X_1 and X_2 respectively. If $F_1 \simeq F_2$, then $|X_1| = |X_2|$. Moreover the same is true if F_1 and F_2 are free groups on X_1 and X_2.*

Proof. Using 2.3.8 write $F_i = \mathrm{Dr}_{x \in X_i} \langle a_{x,i} \rangle$ where $\langle a_{x,i} \rangle$ is infinite cyclic. Now $F_1 \simeq F_2$ implies that $F_1/F_1^2 \simeq F_2/F_2^2$. But F_i/F_i^2 is a vector space over the field GF(2) with basis $\{a_{x,i}F_i^2 \mid x \in X_i\}$; its dimension is therefore $|X_i|$. Since isomorphic vector spaces have the same dimension, $|X_1| = |X_2|$.

Finally, if F_1 and F_2 are free on X_1 and X_2, then $F_1 \simeq F_2$ implies that $F_1/F_1' \simeq F_2/F_2'$, whence $|X_1| = |X_2|$. □

EXERCISES 2.3

1. Prove that a subgroup which is generated by W-marginal subgroups is itself W-marginal.
2. If $W = \{x^2\}$, identify $W^*(G)$.
3. Let G be the multiplicative group of all complex 2^nth roots of unity, $n = 0, 1, 2, \dots$. Prove that 1 and G are the only verbal subgroups of G, but that every subgroup is marginal. Show also that G has a fully-invariant subgroup which is not verbal.
4. Prove that every variety is closed with respect to forming subgroups, images, and subcartesian products.
5. Let $\mathfrak{B}$ be any variety. If G is a $\mathfrak{B}$-group with a normal subgroup N such that G/N is a free $\mathfrak{B}$-group, show that there is a subgroup H such that $G = HN$ and $H \cap N = 1$.
6. A variety is said to be *abelian* if all its members are abelian. Find all the abelian varieties.
7. If $\mathfrak{X}$ is any class of groups, define Var $\mathfrak{X}$ to be the intersection of all varieties that contain $\mathfrak{X}$. Prove that Var $\mathfrak{X}$ is a variety and that it consists of all images of subgroups of cartesian products of $\mathfrak{X}$-groups. Describe Var$(\mathbb{Z}_p)$ and Var$(\mathbb{Z})$ where (G) denotes the class of groups consisting of unit groups and isomorphic images of the group G.
8. Prove that $\mathbb{Q}$ is not a subcartesian product of infinite cyclic groups.
9. If F is a free abelian group, show that F is residually a finite p-group and also that F is residually of prime exponent.
10. Let F be a finite group and let G be a finitely generated group in Var(F) where (F) is the class of all trivial groups and groups isomorphic with F. Prove that G is finite. [*Hint*: Apply Exercises 1.4.2 and 2.3.7.]

CHAPTER 3

Decompositions of a Group

In this chapter we shall study ways in which a group may be decomposed into a set of groups each of which is in some sense of simpler type. This idea, the resolution of a single complex structure into a number of less complicated structures, is encountered in almost all branches of algebra.

3.1. Series and Composition Series

Let G be an operator group with operator domain Ω. An *Ω-series* (of finite length) in G is a finite sequence of Ω-subgroups including 1 and G such that each member of the sequence is a normal subgroup of its successor: thus a series can be written

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_l = G.$$

The G_i are the *terms* of the series and the quotient groups G_{i+1}/G_i are the *factors* of the series. If all the G_i are distinct, the integer l is called the *length* of the series.

Since normality is not a transitive relation (Exercise 1.3.15), the G_i need not be normal subgroups of G. A subgroup which is a term of at least one Ω-series is said to be *Ω-subnormal* in G. Thus H is Ω-subnormal in G if and only if there exist distinct Ω-subgroups $H_0 = H, H_1, \ldots, H_n = G$ such that $H = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$; the latter we call an Ω-series *between* H and G.

When Ω is empty, we shall simply speak of a *series* and a *subnormal subgroup*. If $\Omega = \text{Inn } G$, $\text{Aut } G$, or $\text{End } G$, the terms of an Ω-series are normal, characteristic, or fully-invariant in G and we shall speak of a *normal*

series, a *characteristic series*, or a *fully-invariant series*. Of course the advantage in working with Ω-series is that we shall obtain the theory of such series as special cases.

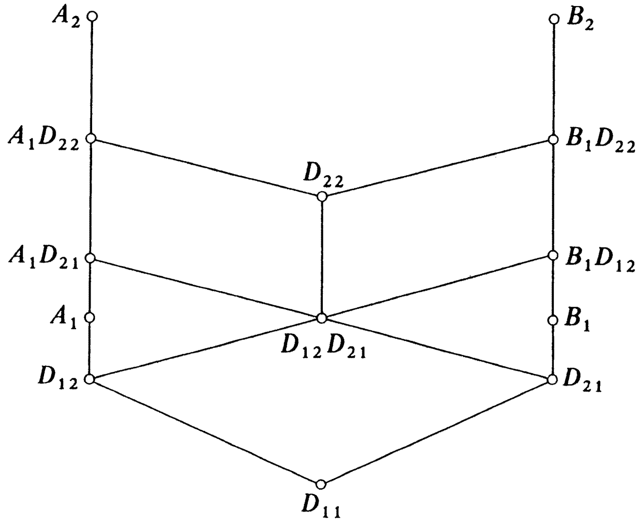
Refinements

Consider the set of all Ω-series of an Ω-group G: there will always be at least one such series, namely $1 \lhd G$. If **S** and **T** are Ω-series of G, call **S** a *refinement* of **T** if every term of **T** is also a term of **S**. If there is at least one term of **S** which is not a term of **T**, then **S** is a *proper refinement* of **T**. Clearly the relation of refinement is a partial ordering of the set of all Ω-series of G.

Isomorphic Series

Two Ω-series **S** and **T** of an Ω-group G are said to be *Ω-isomorphic* if there is a bijection from the set of factors of **S** to the set of factors of **T** such that corresponding factors are Ω-isomorphic. There is a basic result which is useful in dealing with isomorphism of series.

3.1.1 (Zassenhaus's Lemma). *Let A_1, A_2, B_1, B_2 be Ω-subgroups of an Ω-group G such that $A_1 \lhd A_2$ and $B_1 \lhd B_2$. Let $D_{ij} = A_i \cap B_j$. Then $A_1D_{21} \lhd A_1D_{22}$ and $B_1D_{12} \lhd B_1D_{22}$. Furthermore the groups A_1D_{22}/A_1D_{21} and B_1D_{22}/B_1D_{12} are Ω-isomorphic.*



Proof. Since $B_1 \lhd B_2$, we have $D_{21} \lhd D_{22}$. Since also $A_1 \lhd A_2$, it follows that $A_1 D_{21} \lhd A_1 D_{22}$ (Exercise 1.4.3): similarly $B_1 D_{12} \lhd B_1 D_{22}$. Apply the Second Isomorphism Theorem (1.4.4) with $H = D_{22}$ and $N = A_1 D_{21}$, noting that $NH = A_1 D_{22}$ and $N \cap H = D_{12} D_{21}$ by the modular law (1.3.14). The conclusion is that $A_1 D_{22}/A_1 D_{21} \simeq^{\Omega} D_{22}/D_{12} D_{21}$. Similarly $B_1 D_{22}/B_1 D_{12} \simeq^{\Omega} D_{22}/D_{12} D_{21}$, whence the result follows. □

We can now prove the fundamental theorem on refinements.

3.1.2 (The Schreier† Refinement Theorem). *Any two Ω-series of an Ω-group possess Ω-isomorphic refinements.*

Proof. Let $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_l = G$ and $1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G$ be two Ω-series of G. Define $H_{ij} = H_i(H_{i+1} \cap K_j)$ and $K_{ij} = K_j(H_i \cap K_{j+1})$. Apply 3.1.1 with $A_1 = H_i$, $A_2 = H_{i+1}$, $B_1 = K_j$, and $B_2 = K_{j+1}$. The conclusion is that $H_{ij} \lhd H_{ij+1}$, $K_{ij} \lhd K_{i+1j}$, and $H_{ij+1}/H_{ij} \simeq^{\Omega} K_{i+1j}/K_{ij}$. Hence the series $\{H_{ij} | i = 0, \ldots, l-1,\ j = 0, \ldots, m\}$ and $\{K_{ij} | i = 0, \ldots, l,\ j = 0, \ldots, m-1\}$ are Ω-isomorphic refinements of $\{H_i | i = 0, \ldots, l\}$ and $\{K_j | j = 0, \ldots, m\}$ respectively. □

Composition Series

An Ω-series which has no proper refinements is called an Ω-*composition series*. Now not every group has a composition series: for example, any series in $\mathbb{Z}$ must have its smallest nontrivial term infinite cyclic, so it is bound to have a proper refinement. On the other hand, it is clear that we shall arrive at an Ω-composition series of a finite Ω-group if we repeatedly refine any given series.

If Ω is empty, we speak of a *composition series*. When $\Omega = \text{Inn } G$, Aut G, or End G, an Ω-composition series is called a *principal series*, a *principal characteristic series*, or a *principal fully-invariant series* respectively.

It turns out that a composition series can be recognized by the structure of its factors. At this point the concept of an Ω-simple group becomes important. An Ω-group is said to be Ω-*simple* if it is not of order 1 and it has no proper nontrivial normal Ω-subgroups: as usual we speak of a *simple group* if Ω is empty. If G is Ω-simple and $\Omega = \text{Aut } G$, then G is called *characteristically simple*.

3.1.3. *An Ω-series is an Ω-composition series if and only if all its factors are Ω-simple.*

† Otto Schreier (1901–1929).

Proof. If some factor X/Y of an Ω-series of an Ω-group G is not Ω-simple, it possesses a nontrivial normal Ω-group W/Y where $Y < W < X$. Adjunction of W to the series produces a proper refinement, so the initial series is not an Ω-composition series. Conversely, if an Ω-series is not a composition series, it has a proper refinement and there exist consecutive terms $Y < X$ and an Ω-subnormal subgroup W of G lying strictly between Y and X. But then W/Y is Ω-subnormal in X/Y and the latter cannot be Ω-simple. □

We come now to the main theorem on composition series.

3.1.4 (The Jordan–Hölder† Theorem). *If* **S** *is an* Ω*-composition series and* **T** *is any* Ω*-series of an* Ω*-group* G, *then* **T** *has a refinement which is a composition series and is* Ω*-isomorphic with* **S**. *In particular, if* **T** *is a composition series, it is* Ω*-isomorphic with* **S**.

Proof. By 3.1.2 there exist Ω-isomorphic refinements of **S** and **T**. But **S** has no proper refinements, so **S** is Ω-isomorphic with a refinement of **T**. By 3.1.3 this refinement is also an Ω-composition series. □

Thus the factors of an Ω-composition series are independent of the series and constitute a set of invariants of the group, the Ω-*composition factors* of G. Also all Ω-composition series of G have the same length, the Ω-*composition length* of G.

Chain Conditions and Composition Series

Let us consider a partially ordered set Λ with partial order $\leq$. We say that Λ satisfies the *maximal condition* if each nonempty subset Λ_0 contains at least one *maximal element*, that is, an element which does not precede any other element of Λ_0. We also say that Λ satisfies the *ascending chain condition* if there does not exist an infinite properly ascending chain $\lambda_1 < \lambda_2 < \cdots$ in Λ.

In fact these properties are identical. For if a nonempty subset Λ_0 has no maximal element, each element of Λ_0 precedes another element of Λ_0, which permits the construction of an infinite chain $\lambda_1 < \lambda_2 < \cdots$ in Λ. Conversely, if Λ contains an infinite ascending chain $\lambda_1 < \lambda_2 < \cdots$, then plainly $\{\lambda_1, \lambda_2, \dots\}$ has no maximal element.

In an entirely analogous way the *minimal condition* and the *descending chain condition* are defined and may be shown to be identical. The reader should supply the details.

Returning to groups, let us associate with each Ω-group G a set $\mathbf{F}(G)$ of Ω-subgroups such that if $\alpha: G \to H$ is an Ω-isomorphism, $\mathbf{F}(H) = \{S^\alpha \mid S \in \mathbf{F}(G)\}$. For example, $\mathbf{F}(G)$ might consist of all Ω-subgroups or of all Ω-subnormal subgroups of G. Now $\mathbf{F}(G)$ is a partially ordered set with respect to set containment, so we may apply to it the notion of a chain condition.

† Otto Hölder (1859–1937).

Definitions

An Ω-group satisfies the *maximal condition on* **F**-*subgroups* if $\mathbf{F}(G)$ satisfies the maximal condition. Similarly G satisfies the *minimal condition on* **F**-*subgroups* if $\mathbf{F}(G)$ satisfies the minimal condition. These properties are identical with the *ascending chain condition* and the *descending chain condition on* **F**-*subgroups* respectively, the latter being defined as the corresponding chain conditions for the partially ordered set $\mathbf{F}(G)$.

Observe that the hypothesis on **F** guarantees that these are group-theoretical properties in the sense of 2.3. We mention the most important cases.

Examples

(i) $\mathbf{F}(G)$ = the set of all Ω-subgroups of the Ω-groups G. We obtain the *maximal and minimal condition on* Ω-*subgroups*, often denoted by max-Ω and min-Ω. When Ω is empty, we simply write max and min and speak of *the maximal and minimal conditions on subgroups.* If $\Omega = \text{Inn } G$, then max-Ω and min-Ω are denoted by max-n and min-n, the *maximal and minimal conditions on normal subgroups.*

(ii) $\mathbf{F}(G)$ = the set of all Ω-subnormal subgroups: this is the case which concerns us here since the corresponding properties max-Ωs and min-Ωs are intimately related to the question of the existence of a composition series.

3.1.5. *An Ω-group G has an Ω-composition series if and only if it satisfies* max-Ωs *and* min-Ωs.

Proof. Suppose that G has an Ω-composition series of length l but that nevertheless there exists an infinite ascending chain $H_1 < H_2 < \cdots$ of Ω-subnormal subgroups of G. Consider the chain $1 \leq H_1 < H_2 < \cdots < H_{l+1}$: since H_i is Ω-subnormal in G, it is Ω-subnormal in H_{i+1}. Hence our chain can be made into an Ω-series of G by inserting terms of a suitable Ω-series between H_i and H_{i+1} and between H_{l+1} and G. The length of the resulting series is at least $l + 1$ but cannot exceed the composition length by 3.1.4, a contradiction. In a similar manner we may prove that G has min-Ωs.

Now assume that G has max-Ωs and min-Ωs but does not have an Ω-composition series. Apply max-Ωs to the set of proper normal Ω-subgroups of G—note that G does not have order 1—and select a maximal member G_1: then G/G_1 is Ω-simple. Now $G_1 \neq 1$ since G has no Ω-composition series, and by max-Ωs again we may choose a maximal proper normal Ω-subgroup G_2 of G_1. Again G_1/G_2 is Ω-simple and $G_2 \neq 1$. This process cannot terminate, so there is an infinite descending chain of Ω-subnormal subgroups of the form $\cdots < G_2 < G_1 < G_0 = G$, in contradiction to min-Ωs. □

The groups which satisfy max-s and min-s are, therefore, precisely the groups which possess a composition series. By the Jordan–Hölder Theorem the composition factors of such a series are invariants of the group. These are, of course, simple groups. Thus in a real sense the group is constructed from a well-defined set of simple groups by a process of repeated extension. Here a group G is said to be *an extension* of a group N by a group Q if there exists $M \lhd G$ such that $M \simeq N$ and $G/M \simeq Q$.

For example, to construct all finite groups it would be necessary to: (i) construct all finite simple groups; and (ii) construct all extensions of a finite group N by a finite simple group Q. Attractive as this program might seem at first glance, it is fraught with difficulties. The classification of all finite simple groups is an exceedingly difficult problem which has only recently been completed. Moreover, although the problem of constructing all extensions of N by Q is in principle solved in Chapter 11, to decide when two of the constructed extensions are isomorphic is usually a very difficult matter.

Properties of Chain Conditions

We conclude by proving some important results about chain conditions.

3.1.6. *An Ω-group satisfies* max-Ω *if and only if every Ω-subgroup may be finitely generated as an Ω-group.*

Proof. First suppose that G has max-Ω and that H is an Ω-subgroup which cannot be Ω-finitely generated. Let $h_1 \in H$: then $H_1 = \langle h_1 \rangle^\Omega \neq H$ and there exists $h_2 \in H \backslash H_1$. Thus $H_1 < H_2 = \langle h_1, h_2 \rangle^\Omega$ and $H_2 \neq H$. Choose $h_3 \in H \backslash H_2$; then $H_1 < H_2 < H_3 = \langle h_1, h_2, h_3 \rangle^\Omega$, and so on. This process cannot terminate, so it yields an infinite ascending chain of Ω-subgroups $H_1 < H_2 < H_3 < \cdots$; but this is impossible. Conversely assume that each Ω-subgroup is finitely generated, but that nevertheless there is an infinite chain of Ω-subgroups $H_1 < H_2 < \cdots$. Let $H = \bigcup_{i=1,2,\ldots} H_i$: since H is an Ω-subgroup, $H = \langle x_1, \ldots, x_i \rangle^\Omega$ for some finite set of elements $\{x_1, \ldots, x_i\}$. For large enough n each x_i belongs to H_n, so $H = H_n$, which is a contradiction. □

In particular G *satisfies* max *if and only if each subgroup is finitely generated*; also G *satisfies* max-n *if and only if each normal subgroup is the normal closure of a finite subset.*

3.1.7. *Each of the properties* max-Ω, max-Ωs, min-Ω, min-Ωs *is closed with respect to forming extensions. Thus, if $N \lhd G$ and N and G/N have the property in question, then so does G.*

Proof. For example take the case of max-Ωs. Let $N \lhd G$ where G is an Ω-group and N an Ω-subgroup. Suppose that N and G/N both have max-Ωs, but that nevertheless there exists an infinite ascending chain $H_1 < H_2 < \cdots$ of Ω-subnormal subgroups of G. Now $H_i \cap N$ is Ω-subnormal in N and H_iN/N is Ω-subnormal in G/N: hence there is an $r > 0$ such that $H_r \cap N = H_{r+1} \cap N$ and $H_rN = H_{r+1}N$. But Exercise 1.3.16 shows that $H_r = H_{r+1}$. □

In particular 3.1.7 applies to the properties max, max-*n*, max-*s*, min, min-*n*, min-*s*. Now every cyclic group satisfies max since (by Exercise 1.3.6) a nontrivial subgroup has finite index. Hence *every polycyclic group satisfies* max.

It is an unfortunate fact that the properties max-*n* and min-*n* are not inherited by subgroups—see Exercises 3.1.9 and 3.1.10. The following result is therefore of considerable interest.

3.1.8 (Wilson). *If a group G satisfies* min-*n* *and H is a subgroup of G with finite index, then H satisfies* min-*n*.

Proof. Suppose that H does not in fact have min-*n*. Since G/H_G is finite by 1.6.9, the subgroup H_G cannot have min-*n* either. Thus we may as well suppose that $H \lhd G$. Now H does not satisfy min-H, the minimal condition on H-admissible subgroups. By min-*n* it follows that H contains a normal subgroup K of G which is minimal with respect to not satisfying min-H.

Consider the set $\mathscr{S}$ of all finite nonempty subsets X of G with the following property: if

$$K_1 > K_2 > \cdots \tag{1}$$

is an infinite strictly decreasing sequence of H-admissible subgroups of K, then

$$K = K_i^X \tag{2}$$

holds for all i. It is not evident that such subsets exist, so our first concern is to produce one.

Let T be a transversal to H in G; thus $G = HT$. For any chain of the above type we have $K_i \lhd H \lhd G$, and hence $K_i^T \lhd HT = G$. Also $K_i^T \leq K$ since $K \lhd G$. If $K_i^T \neq K$, then K_i^T has the property min-H by minimality of K. But this implies that $K_j = K_{j+1}$ for some $j \geq i$. By this contradiction $K_i^T = K$ for all i and $T \in \mathscr{S}$.

We now select a minimal element of $\mathscr{S}$, say X. If $x \in X$, then $Xx^{-1} \in \mathscr{S}$ because $K \lhd G$. Of course Xx^{-1} is also minimal in $\mathscr{S}$ and it contains 1. Thus we may assume that $1 \in X$. If in fact X contains no other element, then (1) and (2) are inconsistent, so that K has min-H. Consequently the set

$$Y = X \backslash \{1\}$$

is nonempty. Therefore Y does not belong to $\mathscr{S}$ by minimality of X.

It follows that there exists an infinite sequence $K_1 > K_2 > \cdots$ with $K_i \leq K$ and $K_i \lhd H$ such that $K_j^Y \neq K$ for some j. Define

$$L_i = K_i \cap K_i^Y.$$

Now $K_i^g \lhd H^g = H$ for all g in G, so $L_i \lhd H$. Also $L_i \geq L_{i+1}$. Suppose that $L_i = L_{i+1}$; since $X \in \mathcal{S}$, we must have $K = K_{i+1}^X$ and

$$K_i = K_i \cap K_{i+1}^X = K_i \cap (K_{i+1} K_{i+1}^Y) \leq K_{i+1} L_i = K_{i+1},$$

contradicting $K_i > K_{i+1}$. Hence $L_i > L_{i+1}$ for all i. Therefore $L_i^X = K$ for all i, which shows that

$$K_j = K_j \cap L_j^X = K_j \cap (L_j L_j^Y) \leq L_j(K_j \cap K_j^Y) = L_j.$$

Hence $K_j = L_j$. Finally, by definition of L_j we obtain $K_j^Y = K_j^X = K$, a contradiction. □

There is a corresponding theorem for max-n provable by analogous methods (Exercise 3.1.11).

Exercises 3.1

1. Prove the Fundamental Theorem of Arithmetic by applying the Jordan–Hölder Theorem to $\mathbb{Z}_n$.
2. Give an example of an abelian group and a nonabelian group with the same composition factors.
3. Show that neither of the properties max and min implies the other.
4. If G has an Ω-composition series, prove that every Ω-subgroup and Ω-image of G have a composition series.

*5. Prove that the additive group of a vector space is characteristically simple.

6. Prove that for partially ordered sets the descending chain condition is equivalent to the minimal condition.

*7. Show that a group with min is a torsion group.

*8. Let $H\ \Omega$ sn K mean that H is Ω-subnormal in K.
   (a) If $H\ \Omega$ sn $K \leq G$ and L is an Ω-subgroup of G, show that $H \cap L\ \Omega$ sn $K \cap L$.
   (b) If $H\ \Omega$ sn $K \leq G$ and θ is an Ω-homomorphism from G, prove that $H^\theta\ \Omega$ sn K^θ.

*9. Prove that the property max-n is not inherited by normal subgroups, proceeding thus: let A be the additive group of rationals of the form $m2^n$, $m, n \in \mathbb{Z}$, and let $T = \langle t \rangle$ be infinite cyclic. Let t act on A by the rule $at = 2a$. Now consider the group $G = T \ltimes A$.

*10. Prove that the property min-n is not inherited by normal subgroups by using the following construction (due to V.S. Čarin). Let p and q be distinct primes. Let F be the field generated by all p^ith roots of unity over $GF(q)$ where $i = 1, 2, \dots$, and denote by X the multiplicative group of all such roots. Then X acts on the additive group A of F via the field multiplication. Prove that A is a simple X-operator group. Now consider the group $G = X \ltimes A$.

11. If G satisfies max-n, so does every subgroup H with finite index in G (J.S. Wilson). [*Hint*: We can assume that $H \lhd G$. Choose $K \lhd G$ maximal subject to H/K not satisfying max-n. Define $\mathscr{S}$ to be the set of all nonempty finite subsets X such that if $K \leq K_1 < K_2 < \cdots$ is an infinite ascending chain of normal subgroups of H, then $K = (K_i)_X$ for every i. Now proceed as in 3.1.8.]

3.2. Some Simple Groups

We have seen that simple groups are the building blocks out of which groups with a composition series, and in particular finite groups, are constructed. The examples of simple groups which come first to mind are the groups of prime order: these have no proper nontrivial subgroups and they are the only abelian simple groups. In this section we shall give some examples of nonabelian simple groups.

The Simplicity of the Alternating Groups

The first nonabelian simple groups to be discovered were the alternating groups A_n, $n \geq 5$. The simplicity of A_5 was known to Galois and is crucial in showing that the general equation of degree 5 is not solvable by radicals.

3.2.1 (Jordan). *The alternating group A_n is simple if and only if $n \neq 1, 2$, or 4.*

To prove this we shall need a simple fact about 3-cycles in A_n.

3.2.2. *A_n is generated by 3-cycles if $n \geq 3$.*

Proof. Every even permutation is the product of an even number of 2-cycles. Since $(a, b)(a, c) = (a, b, c)$ and $(a, b)(c, d) = (a, b, c)(a, d, c)$, an even permutation is also a product of 3-cycles: finally 3-cycles are even and thus belong to A_n. □

***Proof of* 3.2.1.** In the first place A_4 is not simple since the permutations $(1, 2)(3, 4)$, $(1, 3)(2, 4)$, $(1, 4)(2, 3)$ form together with 1 a normal subgroup. Of course A_1 and A_2 have order 1. On the other hand A_3 is obviously

simple. It remains therefore only to show that A_n is simple if $n \geq 5$. Suppose this is false and there exists a proper nontrivial normal subgroup N.

Assume that N contains a 3-cycle (a, b, c). If (a', b', c') is another 3-cycle and π is a permutation in S_n mapping a to a', b to b', and c to c', then clearly $\pi^{-1}(a, b, c)\pi = (a', b', c')$: if π is odd, we can replace it by the even permutation $\pi(e, f)$ where e, f differ from a', b', c' without disturbing the conjugacy relation. (Here we use the fact that $n \geq 5$.) Hence $(a', b', c') \in N$ and $N = A_n$ by 3.2.2. It follows that N cannot contain a 3-cycle.

Assume now that N contains a permutation π whose (disjoint) cyclic decomposition involves a cycle of length at least 4, say

$$\pi = (a_1, a_2, a_3, a_4, \ldots) \ldots .$$

Then N also contains

$$\pi' = (a_1, a_2, a_3)^{-1}\pi(a_1, a_2, a_3) = (a_2, a_3, a_1, a_4, \ldots) \ldots,$$

so that N contains $\pi^{-1}\pi' = (a_1, a_2, a_4)$: notice that the other cycles cancel here. This is impossible, so nontrivial elements of N must have cyclic decompositions involving cycles of lengths 2 or 3. Moreover such elements cannot involve just one 3-cycle—otherwise by squaring we would obtain a 3-cycle in N.

Assume that N contains a permutation $\pi = (a, b, c)(a', b', c') \ldots$ (with disjoint cycles). Then N contains

$$\pi' = (a', b', c)^{-1}\pi(a', b', c) = (a, b, a')(c, c', b') \ldots$$

and hence $\pi\pi' = (a, a', c, b, c') \ldots$, which is impossible. Hence each element of N is a product of an even number of disjoint 2-cycles.

If $\pi = (a, b)(a', b') \in N$, then N contains $\pi' = (a, c, b)^{-1}\pi(a, c, b) = (a, c)(a', b')$ for all c unaffected by π. Hence N contains $\pi\pi' = (a, b, c)$. It follows that if $1 \neq \pi \in N$, then $\pi = (a_1, b_1)(a_2, b_2)(a_3, b_3)(a_4, b_4) \ldots$, the number of 2-cycles being at least 4. But then N will also contain

$$\pi' = (a_3, b_2)(a_2, b_1)\pi(a_2, b_1)(a_3, b_2) = (a_1, a_2)(a_3, b_1)(b_2, b_3)(a_4, b_4) \ldots$$

and hence $\pi\pi' = (a_1, a_3, b_2)(a_2, b_3, b_1)$, our final contradiction. □

Using this result it is easy to find all normal subgroups of the symmetric group S_n.

3.2.3. *If $n \neq 4$, the only normal subgroups of S_n are 1, A_n, and S_n. Furthermore $1 \lhd A_n \lhd S_n$ is the only composition series of S_n.*

Proof. We can assume that $n \geq 3$. Let $1 \neq N \lhd S_n$; then $N \cap A_n \lhd A_n$, so by 3.2.1 we must have either $A_n \leq N$ or $A_n \cap N = 1$. Since $|S_n : A_n| = 2$, the former implies that $N = A_n$ or S_n. Suppose that $N \cap A_n = 1$; then $S_n = A_n N$ and therefore $S_n = A_n \times N$, so that N lies in $\zeta(S_n)$. But $\zeta(S_n) = 1$ since each conjugacy class of S_n consists of all permutations of some fixed cycle type. □

Examples of infinite simple groups may be found by using the following elementary result.

3.2.4. *If the group G is the union of a chain $\{G_\lambda | \lambda \in \Lambda\}$ of simple subgroups, then G is simple.*

Proof. Let $1 \neq N \lhd G$. Then $N \cap G_\lambda \neq 1$ for some λ and hence $N \cap G_\mu \neq 1$ for all $G_\mu \geq G_\lambda$. But $N \cap G_\mu \lhd G_\mu$ and G_μ is simple, so $G_\mu \leq N$ and $N = G$. □

For example let S be the group of all *finitary* permutations of $\{1, 2, 3, \dots\}$, that is, all permutations which move only a finite number of the symbols. Then define $S(n)$ to be the stabilizer in S of $\{n+1, n+2, \dots\}$. Plainly $S_n \simeq S(n)$: let $A(n)$ be the image of A_n under the isomorphism. Then $A(1) = A(2) < A(3) < \cdots$ and $A = \bigcup_{n=5,6,\dots} A(n)$ is an infinite simple group by 3.2.4. This is called the *infinite alternating group.*

The Simplicity of the Projective Special Linear Groups

Let R be a commutative ring with identity. Recall that $\mathrm{GL}(n, R)$ is the general linear group of degree n over R and $\mathrm{SL}(n, R)$ is the special linear group, the subgroup of all A in $\mathrm{GL}(n, R)$ such that $\det A = 1$.

3.2.5. *The centralizer of* $\mathrm{SL}(n, R)$ *in* $\mathrm{GL}(n, R)$ *is the group of nonzero scalar matrices $a1_n$, $a \in R^*$.*

Proof. Clearly a scalar matrix will commute with any matrix in $\mathrm{GL}(n, R)$. Conversely let $A = (a_{ij})$ belong to the centralizer of $\mathrm{SL}(n, R)$ in $\mathrm{GL}(n, F)$. Write E_{ij} for the elementary $n \times n$ matrix with 1 in the (i, j)th position and 0 elsewhere. Now $1 + E_{ij} \in \mathrm{SL}(n, R)$ if $i \neq j$, so A and $1 + E_{ij}$ commute, whence $AE_{ij} = E_{ij}A$. The (k, j)th coefficient of AE_{ij} is a_{ki} while that of $E_{ij}A$ is 0 if $k \neq i$ and is a_{jj} otherwise. Hence $a_{ki} = 0$ if $k \neq i$ and $a_{ii} = a_{jj}$, which shows that A is scalar. □

3.2.6. *The center of* $\mathrm{GL}(n, R)$ *is the group of nonzero scalar matrices $a1_n$. The center of* $\mathrm{SL}(n, R)$ *is the group of scalar matrices $a1_n$ where $a^n = 1$.*

This follows at once from 3.2.5.

The *projective general linear group* of degree n over the ring R is defined to be

$$\mathrm{PGL}(n, R) = \mathrm{GL}(n, R)/\zeta(\mathrm{GL}(n, R))$$

and the *projective special linear group* is

$$\mathrm{PSL}(n, R) = \mathrm{SL}(n, R)/\zeta(\mathrm{SL}(n, R)) = \mathrm{SL}(n, R)/\mathrm{SL}(n, R) \cap \zeta(\mathrm{GL}(n, R)).$$

In case $R = \mathrm{GF}(q)$, the following notation is used:

$$\mathrm{GL}(n, q), \quad \mathrm{PGL}(n, q), \quad \mathrm{SL}(n, q), \quad \mathrm{PSL}(n, q).$$

Let us compute the orders of these groups.

3.2.7.

(i) $|\mathrm{GL}(n, q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$.
(ii) $|\mathrm{SL}(n, q)| = |\mathrm{GL}(n, q)|/(q - 1) = |\mathrm{PGL}(n, q)|$.
(iii) $|\mathrm{PSL}(n, q)| = |\mathrm{GL}(n, q)|/(q - 1)d$ where $d = \gcd(n, q - 1)$.

Proof. (i) In forming a matrix in $\mathrm{GL}(n, q)$ we may choose the first row in $q^n - 1$ ways, a row of zeros not being allowed, the second row in $q^n - q$ ways, no multiple of the first row being allowed, the third row in $q^n - q^2$ ways, no linear combination of the first two rows being allowed, and so on. Multiplying these numbers together we obtain the order of $\mathrm{GL}(n, q)$.

(ii) $A \mapsto \det A$ is an epimorphism from $\mathrm{GL}(n, q)$ to $\mathrm{GF}(q)^*$ whose kernel is $\mathrm{SL}(n, q)$. Since $|GF(q)^*| = q - 1$, the formula for $|\mathrm{SL}(n, q)|$ comes directly from the First Isomorphism Theorem. The order of $\mathrm{PGL}(n, q)$ follows from 3.2.6.

(iii) follows from 3.2.6 and the fact that the number of solutions in $\mathrm{GF}(q)$ of $a^n = 1$ is $(n, q - 1)$: keep in mind here that $\mathrm{GF}(q)^*$ is cyclic of order $q - 1$. □

We note in passing how the projective linear groups arise in geometry. Let V be an $(n + 1)$-dimensional vector space over a field F. We shall say that two nonzero vectors in V are *equivalent* if one is a nonzero multiple of the other: clearly this is an equivalence relation on $V \backslash \{0_V\}$. Let $\tilde{v}$ denote the equivalence class to which v belongs and let $\tilde{V}$ be the set of all $\tilde{v}$ where $v \neq 0$. Then $\tilde{V}$ is a *projective space* of dimension n over F. If α: $V \to V$ is an F-isomorphism, there is an induced *collineation* $\tilde{\alpha}$: $\tilde{V} \to \tilde{V}$ defined by $\tilde{v}\tilde{\alpha} = \widetilde{v\alpha}$. Moreover it is easy to see that $\alpha \mapsto \tilde{\alpha}$ is an epimorphism from $\mathrm{GL}(V)$ to $\mathrm{PGL}(\tilde{V})$, the group of all collineations of $\tilde{V}$; the kernel consists of all nonzero scalar linear transformations. Thus the group of collineations is isomorphic with $\mathrm{PGL}(n + 1, F)$.

Our major goal in this section is the following theorem.

3.2.8. *Let F be a field and let N be a normal subgroup of* $\mathrm{SL}(n, F)$ *which is not contained in the center. If either $n > 2$ or $n = 2$ and $|F| > 3$, then $N =$* $\mathrm{SL}(n, F)$.

This has the immediate corollary.

3.2.9 (Jordan, Dickson†). *If either $n > 2$ or $n = 2$ and $|F| > 3$, then* $\mathrm{PSL}(n, F)$ *is simple.*

† Leonard Eugene Dickson (1874–1954).

Before proving 3.2.8 we shall develop some matrix theory.

If $0 \neq a \in F$, a matrix of the form $1 + aE_{ij}$ where $i \neq j$ is called a *transvection*: it differs from the identity matrix only in that there is an a in the (i, j)th position. The transvections lie in $\mathrm{SL}(n, F)$ and play a role similar to that of the 3-cycles in A_n. Their importance arises from the fact that left multiplication of a matrix by $1 + aE_{ij}$ has the effect of adding a times the jth row onto the ith row, a so-called *row operation.*

3.2.10. *The transvections generate* $\mathrm{SL}(n, F)$ *if* $n > 1$.

Proof. Let $A \in \mathrm{SL}(n, F)$. We reduce A to 1_n by row operations. Adding a row to the second row if necessary, we may assume that $a_{21} \neq 0$. Add $a_{21}^{-1}(1 - a_{11})$ times the second row onto the first row to get 1 in the $(1, 1)$th position. Subtracting multiples of the first row we can get 0's in the first column below the diagonal. The $(1, 1)$th minor belongs to $\mathrm{SL}(n - 1, F)$ and may be treated similarly until we obtain a matrix with 1's on the diagonal and 0's below. Further row operations reduce the matrix to the identity. Hence $T_k T_{k-1} \cdots T_1 A = 1_n$ for certain transvections T_i, and $A = T_1^{-1} \cdots T_{k-1}^{-1} T_k^{-1}$: of course each T_i^{-1} is a transvection and every transvection belongs to $\mathrm{SL}(n, F)$. □

3.2.11. *If* $n > 2$, *any two transvections are conjugate in* $\mathrm{SL}(n, F)$.

Proof. Consider first the transvections $1 + aE_{ij}$ and $1 + bE_{ij}$ and put $c = a^{-1}b$. Let D be the diagonal $n \times n$ matrix with 1 in the (i, i)th position, c in the (j, j)th position, c^{-1} in some other diagonal position and 1 elsewhere on the diagonal. Then $D \in \mathrm{SL}(n, F)$ and $D^{-1}(1 + aE_{ij})D = 1 + bE_{ij}$. Now consider transvections $1 + aE_{ij}$ and $1 + aE_{rj}$, $i \neq r$. Let P be the $n \times n$ matrix which differs from 1_n only in that there is a 1 in position (i, r), a -1 in position (r, i) and 0's in positions (i, i) and (r, r); then $P \in \mathrm{SL}(n, F)$. We calculate that $P^{-1}(1 + aE_{ij})P = 1 + aE_{rj}$ where $j \neq i, r$. Similarly $Q^{-1}(1 + aE_{rj})Q = 1 + aE_{rs}$ where Q is a matrix of similar type. It follows that all transvections are conjugate in $\mathrm{SL}(n, F)$. □

We remind the reader of the *rational canonical form* of a matrix $A \in \mathrm{SL}(n, F)$: we shall need to know that A is similar (that is, conjugate in $\mathrm{GL}(n, F)$) to a block matrix

$$\begin{bmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & M_r \end{bmatrix},$$

where the M_i are *companion matrices*, of the form

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ a_1 & a_2 & a_3 & \dots & a_{s-1} & a_s \end{bmatrix}.$$

Our proof of 3.2.8 relies on matrix calculations and will be accomplished in three steps.

3.2.12. *If a normal subgroup N of* SL(2, F) *contains a transvection, then* $N =$ SL(2, F).

Proof. Let $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in N$ where $a \neq 0$. It is sufficient to prove that $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N$ for all $x \in F$. For if this has been done, N will contain

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -x & 1 \end{pmatrix},$$

and by 3.2.10 we obtain $N = \mathrm{SL}(2, F)$. Hence we may assume that $|F| > 2$.

Conjugating $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ by $\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}$, we get $\begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix}$. Therefore N contains the matrix

$$\begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & ay^2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a(x^2 - y^2) \\ 0 & 1 \end{pmatrix} \tag{3}$$

for all $x, y \in F$. If F has characteristic different from 2, then $b = (2^{-1}(b + 1))^2 - (2^{-1}(b - 1))^2$, so every element of F is the difference of two squares and the result follows from (3).

We assume henceforth that F has characteristic 2. At any rate N contains $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ where $a^{-1}r$ is a square in F. Conjugate these matrices by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ to obtain $\begin{pmatrix} 1 & 0 \\ -r & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}$ respectively. Hence N contains

$$\begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -r & 1 \end{pmatrix} = \begin{pmatrix} 1 - mr & m \\ amr - a - r & 1 - am \end{pmatrix},$$

where $a^{-1}m$ is a square. Assume that we can choose r and m so that $amr = a + r$. Then N contains for arbitrary y

$$\left[\begin{pmatrix} 1 - mr & m \\ 0 & 1 - am \end{pmatrix}, \begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & my(r - a)(1 - mr)^{-1} \\ 0 & 1 \end{pmatrix}. \tag{4}$$

Choose $l \in F^*$ so that $l^4 \neq 1$: this exists since if all fourth powers in F^* were 1, we should have $|F| = 3$ or 5. Define $m = a^{-1}(1 + l^{-2})$ and $r = al^2$: these satisfy $amr = a + r$ and $a^{-1}m = (a^{-1}(1 + l^{-1}))^2$, so they are proper choices for r and m. Then $my(r - a)(1 - mr)^{-1} = y(l^{-4} - 1)$, which ranges over all of F as y varies. The result now follows from (4). □

3.2.13. *Let N be a normal subgroup of* SL(2, F) *not contained in the center and let $|F| > 3$. Then $N =$* SL(2, F).

Proof. Since N can be replaced by a conjugate in GL(n, F) if necessary, we may suppose that N contains a noncentral element A which is in rational canonical form. By 3.2.12 we can assume that N does not contain a transvection.

First of all suppose that $A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ where $a \neq a^{-1}$. If $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, then N must contain the commutator $[A, B] = A^{-1}B^{-1}AB = \begin{pmatrix} 1 & 1 - a^{-2} \\ 0 & 1 \end{pmatrix}$; this is a transvection since $a^2 \neq 1$.

It follows that A must be of the form $\begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}$. Here b equals -1 since $\det A = 1$. The commutator of A^{-1} and $\begin{pmatrix} 1 & -x^2 \\ 0 & 1 \end{pmatrix}$ equals $\begin{pmatrix} 1 & -x^2 \\ -x^2 & 1 + x^4 \end{pmatrix}$ and belongs to N for all x in F. Conjugation of this by the matrix $\begin{pmatrix} x^{-1} & -x^{-1} \\ 0 & x \end{pmatrix}$ gives $\begin{pmatrix} 0 & 1 \\ -1 & 2 + x^4 \end{pmatrix}$. Hence N contains for all nonzero x and y the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 2 + x^4 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 2 + y^4 \end{pmatrix} = \begin{pmatrix} 1 & x^4 - y^4 \\ 0 & 1 \end{pmatrix}.$$

Since N contains no transvections, the fourth power of every nonzero element of F equals 1. But the polynomial $t^4 - 1$ has at most four roots in F. Hence $|F| = q$ is finite and $q - 1 \leq 4$. Since $q > 3$ by hypothesis, q must equal 5. This case requires a special argument.

We know that N contains $\begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix}$, by putting $x = 1$ in the above. It also contains the commutator of $\begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix}^{-1} = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$, which equals $\begin{pmatrix} 1 & -2 \\ -2 & 0 \end{pmatrix}$ since $q = 5$. Conjugate the latter by $\begin{pmatrix} 2 & -1 \\ -2 & -1 \end{pmatrix}$—which belongs to SL(2, 5)—to get $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ in N. Finally N contains $\begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, a transvection. □

***Proof of* 3.2.8.** In view of 3.2.13 we may assume that $n > 2$. By 3.2.11 all transvections are conjugate in $SL(n, F)$; hence it is enough to produce a transvection in N.

Let A be a noncentral element of N, which may be assumed to be in rational canonical form. Suppose that all the companion matrices of A are 1×1; then A consists of blocks $a_i 1_{n_i}$, $i = 1, \ldots, k$, lying on the diagonal: here of course $a_i \neq a_j$ if $i \neq j$. Since A is not central, k must exceed 1. Then N contains $[A, 1 + E_{1,n_1+n_2}] = 1 + (1 - a_1^{-1}a_2)E_{1,n_1+n_2}$, a transvection.

Hence we can suppose that some companion matrix of A—say the first one—has degree $r > 1$. Then

$$A = \begin{pmatrix} \bar{A} & 0 \\ 0 & * \end{pmatrix} \quad \text{where} \quad \bar{A} = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ a_1 & a_2 & a_3 & \ldots & a_r \end{bmatrix}_{r \times r}, \qquad a_1 \neq 0.$$

If $r > 2$, then N contains $[A, 1 - E_{r1}] = 1 + a_1^{-1}E_{12} - E_{r1}$. Hence N contains $[1 + a_1^{-1}E_{12} - E_{r1}, 1 - E_{r1}] = 1 + a_1^{-1}E_{r2}$, a transvection.

Now let $r = 2$ and write $\bar{A} = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$, $a \neq 0$. Then some element of $SL(2, F)$ does not commute with $\bar{A}$. On commuting a suitable matrix with A we find that N contains $\begin{pmatrix} B & 0 \\ 0 & 1_{n-2} \end{pmatrix}$ where $B \neq 1_2$. If B is scalar, it must equal -1_2 since $\det B = 1$; in this event F cannot have characteristic 2 and N contains the commutator of $\begin{pmatrix} -1_2 & 0 \\ 0 & 1_{n-2} \end{pmatrix}$ with $1 + E_{23}$, which equals the transvection $1 + 2E_{23}$. Otherwise we may suppose that B has the form $\begin{pmatrix} 0 & 1 \\ -1 & c \end{pmatrix}$. Then N contains the commutator of $1 - E_{13}$ and $\begin{pmatrix} B & 0 \\ 0 & 1_{n-2} \end{pmatrix}$, which equals

$$1 + (1 - c)E_{13} - E_{23}.$$

Finally, commuting this with $1 + E_{12}$, we obtain $1 + E_{13}$ in N. □

Discussion of Results. By 3.2.7 the groups $PSL(2, 2)$ and $PSL(2, 3)$ have orders 6 and 12; there exist no simple groups of these order, and in fact it is easy to see that $PSL(2, 2) \simeq S_3$ and $PSL(2, 3) \simeq A_4$. Thus the cases $n = 2$ and $|F| = 2$ or 3 are genuine exceptions to 3.2.8 and 3.2.9.

$PSL(2, 4)$ and $PSL(2, 5)$ both have order 60. Since any simple group of order 60 is isomorphic with A_5 (Exercise 1.6.12), we have $PSL(2, 4) \simeq A_5 \simeq PSL(2, 5)$. But $PSL(2, 7)$ has order 168, not the order of an alternating group: hence this is a new simple group.

$PSL(3, 4)$ is a simple group of order $20{,}160 = \frac{1}{2}(8!)$. However $PSL(3, 4)$ is not isomorphic with A_8; for it can be demonstrated that $PSL(3, 4)$ has no

elements of order 15, unlike A_8 which has (1, 2, 3, 4, 5)(6, 7, 8)—see Exercise 3.2.6. Consequently *there are two nonisomorphic simple groups of order* 20,160.

More Simple Groups

In fact the projective special linear groups form just one of several infinite families of finite nonabelian simple groups, the so-called *groups of Lie type*, which arise as groups of automorphisms of simple Lie algebras. Since we cannot go into details here, the interested reader is referred to [b9].

Apart from the alternating groups and the groups of Lie type, there are twenty-six isolated simple groups. These are the so-called *sporadic groups*. The largest of them, the "Monster," has order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

or approximately 8×10^{53}. The best known of the sporadic groups are the five groups discovered by Mathieu† over a hundred years ago. These will be discussed in Chapter 7.

It is now generally believed that the classification of finite nonabelian simple groups is complete, and that the only groups of this type are the alternating groups, the groups of Lie type and the twenty-six sporadic groups. However a complete proof has not yet been written down, and it would probably extend to several thousand printed pages. For a detailed account of the classification see [b27].

Exercises 3.2

1. Find all the compositions series of S_4.
2. If S is the group of all finitary permutations of the set $\{1, 2, 3, \dots\}$ and A is the alternating subgroup, prove that $1 \lhd A \lhd S$ is the only composition series of S.
3. Prove that PGL(2, $\mathbb{C}$) is isomorphic with the group of all linear fractional transformations of $\mathbb{C}$ (see 2.1).
4. Show that transvections in SL(2, F) need not be conjugate.
5. Prove that PSL(2, 2) $\simeq S_3$ and PSL(2, 3) $\simeq A_4$.
6. Prove that PSL(3, 4) has no element of order 15, so that PSL(3, 4) is not isomorphic with A_8. [*Hint*: Suppose there is such an element: consider the possible rational canonical forms of a preimage in SL(3, 4): see also [b57].]
7. Let G be a finitely generated group not of order 1. By invoking Zorn's Lemma prove that G contains a maximal (proper) normal subgroup. Deduce that G has a quotient group which is a finitely generated simple group.

† Émile Léonard Mathieu (1835–1890).

The next two exercises constitute G. Higman's construction of a finitely generated infinite simple group.

8. Suppose that $H = \langle x, y, z, t\rangle$ is a finite group in which the following relations hold: $y^x = y^2$, $z^y = z^2$, $t^z = t^2$, and $x^t = x^2$. Prove that $H = 1$. [*Hint*: Let i, j, k, l be the orders of x, y, z, t: show that $j|2^i - 1$, $k|2^j - 1$ etc. Using the fact that if $n > 1$, the smallest prime divisor of $2^n - 1$ exceeds the smallest prime divisor of n, show that $i = j = k = l = 1$.]

9. Let G be the group with generators x, y, z, t and relations $y^x = y^2$, $z^y = z^2$, $t^z = t^2$, and $x^t = x^2$. Prove that G has a quotient group which is a finitely generated infinite simple group. (It may be assumed that $G \neq 1$: see Exercise 6.4.15.)

10. Let q be an odd prime power greater than 3. Prove that $SL(2, q)$ equals its derived subgroup.

3.3. Direct Decompositions

We have considered one way of decomposing a group, by resolving it into its composition factors. Another and more precise way would be to express the group as a direct product of factors that themselves cannot be decomposed into a direct product. One disadvantage of this approach is that the indecomposable factors are much less well understood than the simple groups that arise from a composition series.

Let G be a group with operator domain Ω. An Ω-subgroup H is called an *Ω-direct factor* of G if there exists an Ω-subgroup K such that $G = H \times K$; then K is called an *Ω-direct complement* of H in G. If there are no proper nontrivial Ω-direct factors of G, then G is said to be *Ω-indecomposable* (or just *indecomposable* if $\Omega = \varnothing$). Clearly every Ω-simple group is Ω-indecomposable: however a cyclic group of order p^2 where p is prime is an example of an indecomposable group which is not simple.

We shall consider chain conditions on the set of direct factors of a group.

3.3.1. *For groups with operator domain Ω the maximal and minimal conditions on Ω-direct factors are equivalent properties.*

Proof. Assume that G is an Ω-group satisfying the minimal condition on Ω-direct factors: let $\mathscr{S}$ be a nonempty set of Ω-direct factors of G. We will show that $\mathscr{S}$ has a maximal element, so that G satisfies the maximal condition on Ω-direct factors.

Let $\mathscr{T}$ be the set of all Ω-subgroups of G which are direct complements of at least one element of $\mathscr{S}$. Then $\mathscr{T}$ has a minimal element N and $G = M \times N$ for some $M \in \mathscr{S}$. If M is not maximal in $\mathscr{S}$, there exists $M_1 \in \mathscr{S}$ such that $M < M_1$: then $G = M_1 \times N_1$ for some $N_1 \in \mathscr{T}$. Now $M_1 = M_1 \cap (M \times N) = M \times (M_1 \cap N)$, whence $G = M_1 \times N_1 = M \times N_1 \times$

$(M_1 \cap N)$. Intersecting with N we obtain $N = N_2 \times (M_1 \cap N)$ where $N_2 = (M \times N_1) \cap N$. Hence $G = M \times N = (M \times (M_1 \cap N)) \times N_2 = M_1 \times N_2$. It follows that $N_2 \in \mathscr{T}$ and hence that $N_2 = N$ by minimality of N in $\mathscr{T}$. Therefore $N \leq M \times N_1$ and $G = M \times N = M \times N_1 = M_1 \times N_1$. Since $M \leq M_1$, we get $M = M_1$, a contradiction. The converse implication is proved in an entirely analogous way. □

Remak Decompositions

The significance of the equivalent conditions of 3.3.1 is that they guarantee that an Ω-group may be expressed as a direct product of finitely many nontrivial Ω-indecomposable subgroups: such a direct decomposition is called a *Remak*† *decomposition.*

3.3.2 (Remak). *If an Ω-group G has the minimal condition on Ω-direct factors, it has a Remak decomposition.*

Proof. Assume that G has no Remak decomposition. Then G is certainly Ω-decomposable, so the set $\mathscr{S}$ of all proper nontrivial Ω-direct factors of G is not empty. Choose a minimal element G_1 of $\mathscr{S}$ and write $G = G_1 \times H_1$. Then G_1 is Ω-indecomposable by minimality. Clearly H_1 inherits the minimal condition from G and cannot be indecomposable. Hence $H_1 = G_2 \times H_2 > G_2$ where G_2 is Ω-indecomposable, and $G = G_1 \times G_2 \times H_2$. Repetition of this procedure leads to an infinite descending chain $H_1 > H_2 > \cdots$ of Ω-direct factors of G, which cannot exist. □

Projections and Direct Decompositions

Our principal aim is to study the question of the uniqueness of the direct factors in a Remak decomposition. For this we need to analyze in greater detail the notion of a direct decomposition.

An *Ω-projection* of an Ω-group G is a normal idempotent Ω-endomorphism, that is, an Ω-endomorphism $\pi: G \to G$ such that $\pi = \pi^2$ which commutes with all inner automorphisms of G. Thus G^π is a normal Ω-subgroup of G. Such endomorphisms arise whenever one has a direct decomposition.

Let $G = G_1 \times \cdots \times G_r$ be an Ω-direct decomposition of G; then each g in G is uniquely expressible in the form $g = g_1 \cdots g_r$ with $g_i \in G_i$. The endomorphism π_i defined by $g^{\pi_i} = g_i$ is an Ω-projection of G: for clearly $\pi_i^2 = \pi_i$ and $(h^{-1}gh)^{\pi_i} = (h^{\pi_i})^{-1}g^{\pi_i}h^{\pi_i} = h^{-1}g^{\pi_i}h$ for all h in G. In addition $g =$

† Robert Remak (1888–194?).

$g_1 \cdots g_r = g^{\pi_1 + \cdots + \pi_r}$ and $(g^{\pi_i})^{\pi_j} = 1$ if $i \neq j$. Thus the π_i satisfy the conditions

$$\left.\begin{aligned} \pi_1 + \cdots + \pi_r &= 1, \\ \pi_i \pi_j &= 0, \qquad (i \neq j). \end{aligned}\right\} \tag{5}$$

Conversely let there be given normal Ω-endomorphisms $\pi_1, \ldots, \pi_r$ of G satisfying (5). Then $\pi_i = \pi_i(\pi_1 + \cdots + \pi_r) = \pi_i^2$, so that π_i is a projection. Let $G_i = G^{\pi_i}$, a normal Ω-subgroup of G. Now $\pi_1 + \cdots + \pi_r = 1$ implies that $G = G_1 \cdots G_r$. Furthermore, if $g \in G_i \cap \prod_{j \neq i} G_j$, then $g = h^{\pi_i}$ for some h, and $g^{\pi_i} = h^{\pi_i} = g$; but $g^{\pi_i} = 1$ since $G_j^{\pi_i} = 1$ if $i \neq j$, so in fact $g = 1$. Hence $G = G_1 \times \cdots \times G_r$. We have established the following result.

3.3.3. *If G is an Ω-group, there is a bijection between the set of all finite Ω-direct decompositions of G and the set of all finite sets of normal Ω-endomorphisms $\{\pi_1, \ldots, \pi_r\}$ of G satisfying* (5).

The following result is fundamental and has numerous applications.

3.3.4 (Fitting's† Lemma). *Let θ be a normal Ω-endomorphism of an Ω-group G and suppose that G satisfies the maximal and minimal conditions on normal Ω-subgroups. Then there exists a positive integer r such that* $\operatorname{Im} \theta^r = \operatorname{Im} \theta^{r+1} = \cdots$ *and* $\operatorname{Ker} \theta^r = \operatorname{Ker} \theta^{r+1} = \cdots$; *also* $G = (\operatorname{Im} \theta^r) \times (\operatorname{Ker} \theta^r)$.

Proof. Since θ^i is a normal Ω-endomorphism, $\operatorname{Im} \theta^i$ and $\operatorname{Ker} \theta^i$ are normal Ω-subgroups of G. Clearly $\operatorname{Ker} \theta \leq \operatorname{Ker} \theta^2 \leq \cdots$ and $\operatorname{Im} \theta \geq \operatorname{Im} \theta^2 \geq \cdots$, so there is a positive integer r such that $\operatorname{Ker} \theta^r = \operatorname{Ker} \theta^{r+1} = \cdots = K$ and $\operatorname{Im} \theta^r = \operatorname{Im} \theta^{r+1} = \cdots = I$ say. Let $g \in G$: then $g^{\theta^r} \in \operatorname{Im} \theta^r = \operatorname{Im} \theta^{2r}$ and $g^{\theta^r} = h^{\theta^{2r}}$ for some $h \in G$. Hence $h^{-\theta^r} g \in K$ and $g \in IK$, which shows that $G = IK$. Next, if $g \in I \cap K$, then $g = h^{\theta^r}$ with $h \in G$. Therefore $1 = g^{\theta^r} = h^{\theta^{2r}}$, whence $h \in \operatorname{Ker} \theta^{2r} = \operatorname{Ker} \theta^r$ and $g = h^{\theta^r} = 1$. It follows that $G = I \times K$. □

Definition. An endomorphism θ is said to be *nilpotent* if $\theta^r = 0$ for some positive integer r.

3.3.5. *If G is an indecomposable Ω-group with the maximal and minimal conditions on normal Ω-subgroups, a normal Ω-endomorphism of G is either nilpotent or an automorphism.*

Proof. Let θ be a normal Ω-endomorphism of G. By 3.3.4 there is an $r > 0$ such that $G = \operatorname{Im} \theta^r \times \operatorname{Ker} \theta^r$. But G is Ω-indecomposable, so either $\operatorname{Im} \theta^r = 0$ and $\theta^r = 0$ or $G = \operatorname{Im} \theta^r$ and $\operatorname{Ker} \theta^r = 0$; in the latter case θ is an automorphism. □

† Hans Fitting (1906–1938).

An endomorphism α of a group G is called *central* if it operates on $G/\zeta G$ like the identity, that is to say, $g^\alpha \equiv g \bmod \zeta G$ for all g in G.

3.3.6.

(i) *A normal endomorphism which is surjective is central.*
(ii) *A central endomorphism is normal.*

Proof. (i) Let α be a normal surjective endomorphism of G. Then $g^{-1}x^\alpha g = (g^{-1}xg)^\alpha = (g^\alpha)^{-1}x^\alpha g^\alpha$ for all $x, g \in G$. Since $G = G^\alpha$, this implies that $g^\alpha g^{-1} \in \zeta G$ and α is central.

(ii) Let α be a central endomorphism of G and let $x, g \in G$. Then $g^\alpha = gz$ where $z \in \zeta G$. Hence $(g^{-1}xg)^\alpha = (gz)^{-1}x^\alpha gz = g^{-1}x^\alpha g$ and α is normal. □

Hence for automorphisms "normal" and "central" are equivalent.

3.3.7. *Let G be an indecomposable Ω-group with the maximal and minimal conditions on normal Ω-subgroups. Suppose that $\theta_1, \theta_2, \ldots, \theta_k$ are normal Ω-endomorphisms every pair of which is additive (as defined in 1.5). If $\theta_1 + \cdots + \theta_k$ is an automorphism, then so is at least one θ_i.*

Proof. By induction we may assume that $k = 2$ and $\alpha = \theta_1 + \theta_2$ is an automorphism. Put $\psi_i = \alpha^{-1}\theta_i$, so that $\psi_1 + \psi_2 = 1$. Now α is normal since θ_1 and θ_2 are: hence ψ_1 and ψ_2 are normal Ω-endomorphisms. Suppose that neither θ_1 nor θ_2 is an automorphism: then neither ψ_1 nor ψ_2 can be an automorphism. By 3.3.5 both ψ_1 and ψ_2 are nilpotent, so $\psi_1^r = 0 = \psi_2^r$ for some $r > 0$. Now $\psi_1 = 1 - \psi_2$, so $\psi_1\psi_2 = \psi_2\psi_1$. Hence $1 = (\psi_1 + \psi_2)^{2r-1} = \sum_{i=0}^{2r-1}\binom{2r-1}{i}\psi_1^i\psi_2^{2r-i-1}$ by the Binomial Theorem. Since either $i \geq r$ or $2r - i - 1 \geq r$, we have $\psi_1^i\psi_2^{2r-i-1} = 0$ for all i. Hence $1 = 0$, which implies that $G = 1$ and $\theta_1 = 1 = \theta_2$, a contradiction. □

The Krull–Remak–Schmidt Theorem

We come now to the main result of this section.

3.3.8 (Krull, Remak, Schmidt). *Let G be an Ω-group satisfying the maximal and minimal conditions on normal Ω-subgroups. If*

$$G = H_1 \times \cdots \times H_r = K_1 \times \cdots \times K_s$$

are two Remak decompositions of G, then $r = s$ and there is a central Ω-automorphism α of G such that, after suitable relabelling of the K_j's if necessary, $H_i^\alpha = K_i$ and $G = K_1 \times \cdots \times K_k \times H_{k+1} \times \cdots \times H_r$ for $k = 1, \ldots, r$.

Proof. Assume that for some k satisfying $1 \leq k \leq \min(r, s) + 1$ there is a decomposition $G = K_1 \times \cdots \times K_{k-1} \times H_k \times \cdots \times H_r$. Certainly this is true if $k = 1$. Let $\{\sigma_1, \ldots, \sigma_r\}$ be the set of projections specifying this decomposition, and let $\{\pi_1, \ldots, \pi_r\}$ and $\{\rho_1, \ldots, \rho_s\}$ be the corresponding sets of projections for the decompositions $G = H_1 \times \cdots \times H_r$ and $G = K_1 \times \cdots \times K_s$. If $g \in G$, then $g^{\rho_j} \in K_j$ and $g^{\rho_j \sigma_k} = 1$ if $j < k$. Hence $\rho_j \sigma_k = 0$ if $j < k$. Since $\sigma_k = 1\sigma_k = (\rho_1 + \cdots + \rho_s)\sigma_k$, we obtain

$$\rho_k \sigma_k + \rho_{k+1}\sigma_k + \cdots + \rho_s \sigma_k = \sigma_k. \tag{6}$$

Notice that by 1.5.1 these $\rho_j \sigma_k$ are additive.

Consider the restriction of $\rho_j \sigma_k$ to H_k, certainly a normal Ω-endomorphism of H_k. Now H_k inherits the maximal and minimal conditions from G and the restriction of σ_k to H_k is, of course, 1. By (6) and 3.3.7 some $\rho_j \sigma_k$, $k \leq j \leq s$, is an automorphism on H_k. The K_j can be labelled in such a way that $\rho_k \sigma_k$ is an automorphism on H_k.

Let $\bar{K}_k = H_k^{\rho_k} \leq K_k$. Then $\bar{K}_k \lhd K_k$ since ρ_k is normal. If $h^{\rho_k} = 1$ with $h \in H_k$, then $h^{\rho_k \sigma_k} = 1$ and $h = 1$: thus ρ_k maps H_k isomorphically onto $\bar{K}_k$. For the same reason σ_k maps $\bar{K}_k$ monomorphically into H_k. Write $\tilde{K}_k = (\text{Ker}\, \sigma_k) \cap K_k$; then $K_k \cap \tilde{K}_k = 1$. Also, for $x \in K_k$ we have $x^{\sigma_k} \in H_k$ and hence $x^{\sigma_k} = y^{\rho_k \sigma_k}$ for some y in H_k; thus $xy^{-\rho_k} \in \tilde{K}_k$ and $x \in \tilde{K}_k \bar{K}_k$. Consequently $K_k = \tilde{K}_k \times \bar{K}_k$. But K_k is Ω-indecomposable, and $\bar{K}_k \simeq H_k \neq 1$; hence $\tilde{K}_k = 1$ and $\bar{K}_k = K_k$. It follows that ρ_k maps H_k isomorphically to K_k.

Next write $L_k = K_1 \times \cdots \times K_{k-1} \times H_{k+1} \times \cdots \times H_r$, so that $G = L_k \times H_k$. The proof proceeds by showing that $G = L_k \times K_k$. Firstly $L_k^{\sigma_k} = 1$ and $L_k \cap K_k = 1$. Next define $\theta = \sigma_k \rho_k + (1 - \sigma_k)$, a normal Ω-endomorphism of G. If $g = lh$ where $l \in L_k$, $h \in H_k$, then $g^\theta = l^\theta h^\theta = lh^{\rho_k}$ since $l^{\sigma_k} = 1$ and $h^{\sigma_k} = h$. Hence $g^\theta = 1$ implies that $l = 1 = h^{\rho_k}$ (because $L_k \cap K_k = 1$); since ρ_k is monomorphic on H_k, we conclude that $l = 1 = h$. Hence θ is a monomorphism. It follows from Fitting's Lemma that θ is an automorphism and therefore $G = G^\theta \leq G^{\sigma_k \rho_k} G^{1-\sigma_k} \leq K_k \times L_k$ and $G = L_k \times K_k$. This is just to say that $G = K_1 \times \cdots \times K_k \times H_{k+1} \times \cdots \times H_r$.

So far we have proved that there is a decomposition

$$G = K_1 \times \cdots \times K_k \times H_{k+1} \times \cdots \times H_r$$

for $1 \leq k \leq \min(r, s)$, after relabeling the K_j's. If we put $k = \min(r, s)$, it follows that $r = s$. We also saw that ρ_k maps H_k isomorphically to K_k for all k. Define $\alpha = \pi_1 \rho_1 + \cdots + \pi_r \rho_r$, a normal Ω-endomorphism. Now $H_i^\alpha = H_i^{\pi_i \rho_i} = H_i^{\rho_i} = K_i$, so $G^\alpha = G$. By Fitting's Lemma α is an automorphism and by 3.3.6 it is central. □

Uniqueness of Remak Decompositions

The Krull–Remak–Schmidt Theorem guarantees that the factors of a Remak decomposition are unique up to isomorphism. It does not assert

that there is a unique Remak decomposition (up to order of the direct factors). Indeed the Klein 4-group has three such decompositions. We enquire next just when a group has a unique Remak decomposition.

3.3.9. *Let $G = G_1 \times \cdots \times G_r$ be a Remak decomposition of an Ω-group with the maximal and minimal conditions on normal Ω-subgroups. This is the only Remak decomposition of G (up to order of the direct factors) if and only if $G_i^\theta \leq G_i$ for every normal Ω-endomorphism θ of G and $i = 1, 2, \ldots, r$.*

Proof. We can assume that $r > 1$. Since a central Ω-automorphism is normal (by 3.3.6), sufficiency follows from the Krull–Remak–Schmidt Theorem. Conversely assume that $G = G_1 \times \cdots \times G_r$ is the unique Remak decomposition of G and let θ be a normal Ω-endomorphism of G such that $G_1^\theta \nleq G_1$. Let $\{\pi_1, \ldots, \pi_r\}$ be the set of associated projections. Then

$$\theta = \theta\left(\sum_j \pi_j\right) = \sum_j \theta\pi_j,$$

so that $G_1^\theta \leq \prod_j G_1^{\theta\pi_j}$. Since $G_1^\theta \nleq G_1$, there is a $j > 1$ such that $\theta\pi_j \neq 0$. Define $\bar{G}_1 = \{xx^{\theta\pi_j} | x \in G_1\}$. Then it is easy to see that $G_1 \neq \bar{G}_1 \leq G$, and also that $G = \bar{G}_1 \times G_2 \times \cdots \times G_r$ is another Remak decomposition. □

From this a more useful condition for uniqueness can be derived.

3.3.10. *A Remak decomposition $G = G_1 \times \cdots \times G_r$ of an Ω-group with the maximal and minimal conditions on normal Ω-subgroups is unique (up to order of factors) if and only if there exist no nontrivial Ω-homomorphisms from G_i to the center of G_j for any $i \neq j$.*

Proof. We can assume that $r > 1$. If $\theta: G_i \to \zeta(G_j)$ is a nontrivial Ω-homomorphism and π_i is the ith projection, then $\pi_i\theta$ is a normal Ω-endomorphism not preserving G_i. Conversely, if θ is a normal Ω-endomorphism such that $G_i^\theta \nleq G_i$, then for some $j \neq i$ the restriction of $\theta\pi_j$ to G_i is a nontrivial Ω-homomorphism from G_i to G_j. If $g \in G_i$ and $x \in G_j$, then $(g^{\theta\pi_j})^x = (g^x)^{\theta\pi_j} = g^{\theta\pi_j}$ since $\theta\pi_j$ is normal. Consequently $g^{\theta\pi_j} \in \zeta(G_j)$. The result follows from 3.3.9. □

In particular, if $G = G'$ or $\zeta G = 1$, there is a unique Remak decomposition of G.

Direct Products of Simple Groups

One very special type of Remak decomposition is a direct product of finitely many simple groups. Let us call a group Ω-*completely reducible* if it is a direct product of a possibly infinite family of simple groups.

3.3.11. *If an Ω-group G is generated by a set of normal Ω-simple subgroups, it is the direct product of certain of these subgroups. Thus G is Ω-completely reducible.*

Proof. Let $G = \langle G_\lambda | \lambda \in \Lambda \rangle$ where $G_\lambda \lhd G$ and G_λ is Ω-simple. Call a subset Λ' of Λ *independent* if $\langle G_\lambda | \lambda \in \Lambda' \rangle = \mathrm{Dr}_{\lambda \in \Lambda'} G_\lambda$, that is, if

$$G_\lambda \cap \langle G_\mu | \mu \in \Lambda', \mu \neq \lambda \rangle = 1$$

for each λ in Λ'. The set $\mathscr{S}$ of all independent subsets of Λ is nonempty since it contains every one-element subset. Also $\mathscr{S}$ is partially ordered by set containment. If $\{\Lambda_i | i \in I\}$ is a chain in $\mathscr{S}$, the union of the chain belongs to $\mathscr{S}$: for clearly a set is independent if its finite subsets are. By Zorn's Lemma there is a maximal element of $\mathscr{S}$, say M. If $\lambda \in \Lambda \backslash M$, then $M \cup \{\lambda\}$ is not independent. Since M is independent, it follows that $G_\lambda \cap L \neq 1$ where $L = \langle G_\mu | \mu \in M \rangle$. Now $G_\lambda \cap L \lhd G_\lambda$, so $G_\lambda \leq L$ by simplicity of G_λ. Hence $G = L = \mathrm{Dr}_{\mu \in M} G_\mu$. Otherwise $\Lambda = M$ and again $G = \mathrm{Dr}_{\mu \in M} G_\mu$. □

We consider next normal subgroups of completely reducible groups.

3.3.12 (Remak). *Let $G = \mathrm{Dr}_{\lambda \in \Lambda} G_\lambda$ where G_λ is Ω-simple. Suppose that N is a normal Ω-subgroup of G. Then $G = N \times \mathrm{Dr}_{\mu \in M} G_\mu$ for some $M \subseteq \Lambda$. Moreover, if all the G_λ have trivial centre, then N is actually the direct product of certain of the G_λ. In any case N is Ω-completely reducible.*

Proof. If $N = G$, we take M to be empty. Assume that $N \neq G$ and let $\mathbf{S}$ be the set of all subsets Λ' of Λ such that $\langle N, G_\lambda | \lambda \in \Lambda' \rangle = N \times \mathrm{Dr}_{\lambda \in \Lambda'} G_\lambda$. Since $N \neq G$, some G_λ is not contained in N and since $N \cap G_\lambda \lhd G_\lambda$, it follows that $N \cap G_\lambda = 1_\lambda$ and $\{\lambda\} \in \mathbf{S}$. Hence $\mathbf{S}$ is nonempty. As in the previous proof $\mathbf{S}$ has a maximal element M: let $G^* = \langle N, G_\mu | \mu \in M \rangle = N \times \mathrm{Dr}_{\mu \in M} G_\mu$. If $\lambda \in \Lambda \backslash M$, then $M \cup \{\lambda\} \notin \mathbf{S}$, which implies that $G_\lambda \cap G^* \neq 1$ and $G_\lambda \leq G^*$. Hence $G = G^*$ as required. Finally $N \simeq \mathrm{Dr}_{\lambda \in \Lambda \backslash M} G_\lambda$, so that N is completely reducible.

Now assume that each $\zeta(G_\lambda)$ is trivial. Clearly we may factor out any G_λ contained in N. Assume therefore that $N \cap G_\lambda = 1$ for all λ. Then $[N, G_\lambda] \leq N \cap G_\lambda = 1$, so N is contained in the centre of G. But G has trivial center by Exercise 1.5.8; therefore $N = 1$. □

Thus in an Ω-completely reducible group every normal Ω-subgroup is a direct factor. It is interesting that the converse is true: Ω-completely reducible groups are the only ones in which every normal Ω-subgroup is an Ω-direct factor. Indeed a stronger result is true.

3.3.13 (Head). *If every proper normal Ω-subgroup of an Ω-group G is contained in a proper Ω-direct factor of G, then G is Ω-completely reducible.*

Before we can prove this result we must establish a simple lemma which is used constantly in the study of infinite groups. It is just a straightforward application of Zorn's Lemma.

3.3.14. *Let G be an Ω-group, let H be an Ω-subgroup and let x be an element of G such that $x \notin H$. Then there exists an Ω-subgroup K which is maximal with respect to the properties $H \leq K$ and $x \notin K$.*

Proof. Consider the set **S** of all Ω-subgroups containing H but not x. Then **S** is not empty since H is a member. Clearly **S** is partially ordered by inclusion: moreover the union of any chain in **S** is likewise in **S**. By Zorn's Lemma **S** has a maximal element K. □

***Proof of* 3.3.13.** Let N be the subgroup generated by all the Ω-simple normal subgroups of G; then N is completely reducible by 3.3.11. Suppose that $N \neq G$ and let $x \in G \backslash N$. By 3.3.14 there exists a normal Ω-subgroup M which is maximal subject to $N \leq M$ and $x \notin M$. By hypothesis M is contained in a proper Ω-direct factor D, with $G = D \times E$ say. Since $E \neq 1$, we have $x \in M \times E$ by maximality of M. Also $D \cap (M \times E) = M$ by the modular law, so it follows that $x \notin D$. By maximality of M again, $D = M$ and $G = M \times E$. Now let F be a nontrivial normal Ω-subgroup of E: then $F \lhd G$ and $M \times F$, being a proper normal Ω-subgroup of G, lies in a proper Ω-direct factor. But we have shown that M is contained in no proper Ω-direct factor of G except M itself, so we have a contradiction. □

Characteristically Simple Groups

Recall that a group G which is Aut G-simple, that is, which is nontrivial and has no proper nontrivial characteristic subgroups, is called *characteristically simple*. Closely related is the concept of a *minimal normal subgroup* of a group G, by which is understood a *nontrivial* normal subgroup that does not contain a smaller nontrivial normal subgroup of G. It follows at once from 1.5.6 that in any group a minimal normal subgroup is characteristically simple. The subgroup generated by all the minimal normal subgroups of a group G is called the *socle*: should the group fail to have any minimal normal subgroups, as in the case of the infinite cyclic group for example, the socle of G is defined to be 1. Applying 3.3.11 with $\Omega = \text{Inn } G$, we see that the socle of a group is a direct product of minimal normal subgroups.

3.3.15.

(i) *A direct product of isomorphic simple groups is characteristically simple.*
(ii) *A characteristically simple group which has at least one minimal normal subgroup is a direct product of isomorphic simple groups.*

Proof. (i) Let $G = \mathrm{Dr}_{\lambda \in \Lambda} G_\lambda$ where the G_λ are isomorphic simple groups, and let H be a nontrivial characteristic subgroup of G. If the G_λ are nonabelian, 3.3.12 implies that $G = H \times K$ where H and K are direct products of certain G_λ's. But clearly there is an automorphism of G interchanging any two G_λ's. Hence $H = G$. On the other hand, if the G_λ are abelian, then all of them have some prime order p and G is an elementary abelian p-group. The result now follows from Exercise 3.1.5.

(ii) Let N be a minimal normal subgroup of a characteristically simple group G. Then $\langle N^\alpha | \alpha \in \mathrm{Aut}\, G \rangle$ is characteristic in G and hence equals G. Applying 3.3.11 with $\Omega = \mathrm{Inn}\, G$, we conclude that G is the direct product of certain of the N^α including, we may suppose, N itself. If $1 \neq M \lhd N$, then $M \lhd G$ and $M = N$ by minimality of N. Hence N is simple and G is a direct product of isomorphic copies of N. □

In particular *a finite characteristically simple group is a direct product of isomorphic finite simple groups.* On the other hand the additive group of rationals is an example of a characteristically simple group that is *not* completely reducible.

Centerless Completely Reducible Groups

In the sequel a completely reducible group will be called a CR-*group.* The center of a CR-group is the direct product of the abelian factors in the decomposition. Hence a CR-group is *centerless,* that is has trivial center, if and only if it is a direct product of *nonabelian* simple groups. Centerless CR-groups have a very rigid normal structure.

3.3.16. *If $G = \mathrm{Dr}_{\lambda \in \Lambda} G_\lambda$ where each G_λ is a nonabelian simple group, every normal subgroup of G is a direct product of certain G_λ's.*

This follows at once from 3.3.12.

3.3.17. *In any group G there is a unique maximal normal centerless* CR-*subgroup. Moreover this is characteristic in G.*

Proof. Let $\{M_\lambda | \lambda \in \Lambda\}$ be a chain of centerless normal CR-subgroups of G. Let S be a simple direct factor of M_λ. Now if $M_\lambda \leq M_\mu$, then M_λ is a direct factor of M_μ by 3.3.12. Hence $S \lhd M_\mu$ and $S \lhd J = \bigcup_{\mu \in \Lambda} M_\mu$. Consequently J is generated by *normal* nonabelian simple subgroups and 3.3.10 shows that J is a CR-group. By Zorn's Lemma there exists a maximal normal centerless CR-subgroup M. Now let N be any other normal centerless CR-subgroup of G and put $I = M \cap N$, a normal subgroup of G. By 3.3.12 we have $M = M_1 \times I$ for some M_1. If $g \in G$, then $M = M^g = M_1^g \times I = M_1 \times I$. Applying 3.3.12 we conclude that I has a unique complement in M,

$M_1^g = M_1$ and $M_1 \lhd G$. Thus $MN = M_1IN = M_1N = M_1 \times N$ because $M_1 \cap N = M_1 \cap I = 1$. Since M_1 is clearly a centerless CR-group, so is MN and by maximality $N \leq M$. Thus M is the required subgroup. □

The maximal normal centerless CR-subgroup will be called the *centerless* CR-*radical*. While it may in general be trivial, there is a class of groups for which this radical controls the group, *the finite semisimple groups.*

Finite Semisimple Groups

A finite group is called *semisimple* if it has no nontrivial normal abelian subgroups. All centerless CR-groups are semisimple: so are the symmetric groups S_n for $n \geq 5$ (see 3.2.3). We shall describe a classification due to Fitting of finite semisimple groups in terms of simple groups and their outer automorphism groups.

3.3.18.

(i) *If G is a finite semisimple group with centerless* CR-*radical R, then $G \simeq G^*$ where* $\operatorname{Inn} R \leq G^* \leq \operatorname{Aut} R$.
(ii) *Conversely, if R is a finite centerless* CR-*group and* $\operatorname{Inn} R \leq G \leq \operatorname{Aut} R$, *then G is a finite semisimple group whose centerless* CR-*radical is* $\operatorname{Inn} R \simeq R$.

Proof. (i) Let $C = C_G(R)$: We show first that $C = 1$. If $C \neq 1$, there is a minimal normal subgroup N of G contained in C. Now N is characteristically simple, so it is a CR-group by 3.3.15. Also $\zeta N \lhd G$; thus $\zeta N = 1$ by semisimplicity of G. Hence $N \leq R \cap C = \zeta R = 1$, a contradiction. Let $\tau: G \to \operatorname{Aut} R$ be the conjugation homomorphism: thus $g^\tau: r \mapsto g^{-1}rg$. Then $\operatorname{Ker} \tau = C_G(R) = 1$ and $R^\tau = \operatorname{Inn} R$. If $G^* = \operatorname{Im} \tau$, then $\operatorname{Inn} R \leq G^* \leq \operatorname{Aut} R$ and of course $G \simeq G^*$.

(ii) Let $\alpha \in C = C_{\operatorname{Aut} R}(\operatorname{Inn} R)$ and let $\tau: R \to \operatorname{Aut} R$ be the conjugation homomorphism. Then $r^\tau = \alpha^{-1}r^\tau\alpha = (r^\alpha)^\tau$ for all r in R by 1.5.4. Now τ is a monomorphism because $\zeta R = 1$: hence $r = r^\alpha$ for all $r \in R$ and $\alpha = 1$. Consequently $C = 1$. Now suppose that $A \lhd G$ where A is abelian. Then $A \cap \operatorname{Inn} R \lhd \operatorname{Inn} R \simeq R$, a centerless CR-group. Hence $A \cap \operatorname{Inn} R = 1$ and $A \leq C = 1$. It follows that G is semisimple—it is of course finite since R, and hence $\operatorname{Aut} R$, is. Finally, let M be a normal centerless CR-subgroup of G. Then 3.3.17 implies that $(\operatorname{Inn} R)M$ is a CR-group and by 3.3.12 it has $\operatorname{Inn} R$ as a direct factor. Since $C_{\operatorname{Aut} R}(\operatorname{Inn} R) = 1$, this can only mean that $M \leq \operatorname{Inn} R$ and $\operatorname{Inn} R$ is the centerless CR-radical of G. □

Thus to construct all finite semisimple groups with centerless CR-radical isomorphic to R we need to form all groups intermediate between $\operatorname{Inn} R$

and Aut R, in other words all subgroups of Out R. The question now arises: when are two groups constructed in this manner isomorphic?

3.3.19. *Let R be a finite centerless* CR-*group. There is a bijection between the set of isomorphism classes of finite semisimple groups with centerless* CR-*radical isomorphic with R and the set of conjugacy classes of subgroups of* Out R.

Proof. Let $\text{Inn } R \leq G_i \leq \text{Aut } R$, $i = 1, 2$. If G_1 and G_2 are conjugate in Aut R, then clearly $G_1 \simeq G_2$. Conversely let $\alpha: G_1 \to G_2$ be an isomorphism. By 3.3.18 it is enough to prove that G_1 and G_2 are conjugate in Aut R.

Since Inn R is the centerless CR-radical of G_1 and of G_2, we have $(\text{Inn } R)^\alpha = \text{Inn } R$, so the restriction of α to Inn R is an automorphism. Let $\tau: R \to \text{Aut } R$ be the conjugation homomorphism; this is a monomorphism with image Inn R. Hence α determines an automorphism θ of R given by $(r^\theta)^\tau = (r^\tau)^\alpha$, $(r \in R)$.

We shall prove that $g^\alpha = \theta^{-1} g \theta$ for all g in G_1, which will show that $G_2 = \theta^{-1} G_1 \theta$. Let $r \in R$. Keeping in mind that $\theta\tau = \tau\alpha$ and also that $(r^g)^\tau = g^{-1} r^\tau g$ for all g in Aut R, we obtain

$$\begin{aligned}(r^{\theta^{-1}g\theta})^\tau &= ((r^{\theta^{-1}g})^\tau)^\alpha = (g^{-1}(r^{\theta^{-1}})^\tau g)^\alpha \\ &= (g^\alpha)^{-1} r^\tau g^\alpha \\ &= (r^{g^\alpha})^\tau.\end{aligned}$$

Thereore $\theta^{-1} g \theta = g^\alpha$ as claimed. □

Structure of the Automorphism Group of a Centerless CR-group

Our results so far make it of interest to investigate automorphism groups of finite centerless CR-groups. They may be described in terms of automorphism groups of nonabelian simple groups.

3.3.20. *Let R be a finite centerless* CR-*group and write $R = R_1 \times \cdots \times R_k$ where R_i is a direct product of n_i isomorphic copies of a simple group H_i, and H_i and H_j are not isomorphic if $i \neq j$. Then* $\text{Aut } R \simeq \text{Aut } R_1 \times \cdots \times \text{Aut } R_k$ *and* $\text{Aut } R_i \simeq (\text{Aut } H_i) \wr S_{n_i}$ *where in this wreath product* Aut H_i *appears in its right regular representation and the symmetric group S_{n_i} in its natural permutation representation. Moreover these isomorphisms induce isomorphisms* $\text{Out } R \simeq \text{Out } R_1 \times \cdots \times \text{Out } T_k$ *and* $\text{Out } R_i \simeq (\text{Out } H_i) \wr S_{n_i}$.

Proof. Let $\alpha \in \text{Aut } R$: then R_i^α is a direct product of n_i copies of H_i and by 3.3.12 it must equal R_i. Hence each R_i is characteristic in R and α induces an automorphism α_i in R_i by restriction. Clearly $\alpha \mapsto (\alpha_1, \ldots, \alpha_k)$ is an iso-

morphism from Aut R to Aut $R_1 \times \cdots \times$ Aut R_k in which Inn R is mapped to Inn $R_1 \times \cdots \times$ Inn R_k; it therefore induces an isomorphism Out $R \simeq$ Out $R_1 \times \cdots \times$ Out R_k.

In the remainder of the proof we shall suppose for simplicity of notation that R is the direct product of n copies of the simple group H. Let $\alpha \in A =$ Aut R: it follows from 3.3.12 that α permutes the direct factors of R and hence is associated with a permutation $\pi_\alpha \in S_n$: moreover $\alpha \mapsto \pi_\alpha$ is clearly a homomorphism from A to S_n whose kernel K consists of all automorphisms that preserve each of the n direct factors of R. Thus $K \lhd A$ and an element κ of K induces through its action on the ith direct factor of R an automorphism κ_i of H: the mapping $\kappa \mapsto (\kappa_1, \dots, \kappa_n)$ is an isomorphism of K with the n-fold direct product Aut $H \times \cdots \times$ Aut H.

Next if $\pi \in S_n$, there is an associated automorphism α_π of R which simply permutes components: thus if $r \in R$, we have $(r^{\alpha_\pi})_i = r_{i\pi^{-1}}$. Now $(r^{\alpha_{\pi\bar{\pi}}})_i = r_{i(\pi\bar{\pi})^{-1}} = r_{i\bar{\pi}^{-1}\pi^{-1}} = (r^{\alpha_\pi})_{i\bar{\pi}^{-1}} = (r^{\alpha_\pi \alpha_{\bar{\pi}}})_i$, so $\alpha_{\pi\bar{\pi}} = \alpha_\pi \alpha_{\bar{\pi}}$. Hence $\pi \mapsto \alpha_\pi$ is a monomorphism from S_n to A with image $X \simeq S_n$. Clearly $X \cap K = 1$. Also if $\alpha \in A$, then $\alpha_{\pi_\alpha}^{-1}\alpha \in K$, which implies that $\alpha \in XK$. Hence $A = XK$ and A is the semidirect product of K and X.

To prove that $A \simeq (\text{Aut } H) \sim S_n$, it suffices to show that conjugation by α_π in K permutes components in the manner prescribed by π. Let $\kappa \in K$; we need to establish that when $\alpha_\pi^{-1}\kappa\alpha_\pi$ is applied to any r in R, the effect on the ith component is identical with that produced by $\kappa_{i\pi^{-1}}$. We calculate that

$$(r^{\alpha_\pi^{-1}\kappa\alpha_\pi})_i = (r^{\alpha_\pi^{-1}\kappa})_{i\pi^{-1}} = ((r^{\alpha_\pi^{-1}})_{i\pi^{-1}})^{\kappa_{i\pi^{-1}}} = r_i^{\kappa_{i\pi^{-1}}},$$

as required. □

In order to construct all isomorphism classes of finite semisimple groups we must therefore construct all finite nonabelian simple groups H and identify the classes of conjugate subgroups of direct products of wreath products $(\text{Out } H) \sim S_n$. In simple cases the last step can be carried out.

For example, let $H = A_5$; then Aut $H \simeq S_5$ (Exercise 1.6.18), so that Out H is cyclic of order 2. Hence there are two nonisomorphic finite semisimple groups with centerless CR-radical isomorphic with A_5; of course these must be A_5 and S_5. Again $\text{Out}(H \times H) \simeq \mathbb{Z}_2 \sim \mathbb{Z}_2 \simeq D_8$ (by Exercise 1.6.16). Now the group D_8 has eight conjugacy classes of subgroups. Hence there are eight nonisomorphic finite semisimple groups whose centerless CR-radical is isomorphic with $A_5 \times A_5$.

Exercises 3.3

1. Show that the maximal condition on direct factors does not imply the maximal condition on normal subgroups. Do the same for the minimal condition.
2. Prove that S_n is indecomposable.
3. Prove that a central endomorphism of a group leaves every element of the derived subgroup fixed.

4. Prove that the central automorphisms of a group G form a subgroup $\text{Aut}_c\, G$ of $\text{Aut}\, G$.

5. (J.E. Adney and Ti Yen). Let G be a finite group which has no nontrivial abelian direct factors. Prove that $|\text{Aut}_c\, G| = |\text{Hom}(G_{ab}, \zeta G)|$. Deduce that if G has no nontrivial central automorphisms, then $\zeta G \leq G'$. [*Hint*: If $\alpha \in \text{Aut}_c\, G$, define $\theta_\alpha \in \text{Hom}(G_{ab}, \zeta G)$ by $(gG')^\theta = g^{-1}g^\alpha$. Show that $\alpha \mapsto \theta_\alpha$ is a bijection.]

6. Suppose that $A \times B \simeq A \times C$ and that both max-n and min-n hold in these groups. Prove that $B \simeq C$ (so that A may be "canceled"). Show that this conclusion is not generally valid.

7. If G is a finite group and $|G_{ab}|$ and $|\zeta G|$ are coprime, prove that G has a unique Remak decomposition.

8. Let $G = G_1 \times G_2 \times \cdots \times G_k$ be a Remak decomposition of the finite group G. Assume that no two of the G_i are isomorphic. Denote by A the subgroup of all automorphisms of G that leave each G_i invariant. Prove the following:
   (i) $A \simeq \text{Aut}\, G_1 \times \text{Aut}\, G_2 \times \cdots \times \text{Aut}\, G_n$;
   (ii) $\text{Aut}\, G = A\, (\text{Aut}_c\, G)$; and
   (iii) $\text{Aut}\, G = A$ if and only if G has only one Remak decomposition.

9. Find the order of $\text{Aut}(D_8 \times S_3)$ (using Exercise 3.3.8).

10. Let G be a finite group. Show that G is completely reducible if and only if it equals its socle.

11. Identify the socle of an abelian group.

12. Prove that an image of a completely reducible group is completely reducible. Prove also that the corresponding statement for centerless completely reducible groups is true.

13. Let G be a finite semisimple group with centerless CR-radical R. Let θ: $\text{Aut}\, G \to \text{Aut}\, R$ be the restriction map, i.e., α^θ is the restriction of α to R. Show that θ is an injective homomorphism. If G is regarded as a subgroup of $\text{Aut}\, R$ as in 3.3.18, prove that $\text{Im}\, \theta = N_{\text{Aut}\, R}(G)$.

CHAPTER 4

Abelian Groups

The theory of abelian groups is a branch of group theory with a flavor all of its own. Indeed, as László Fuchs has remarked, there are few properties with a more decisive influence on group structure than commutativity.

Throughout this chapter we shall be concerned only with abelian groups and we shall therefore write all groups *additively*.

4.1. Torsion Groups and Divisible Groups

Let G be an abelian group and let x, y be elements of G with finite orders m, n respectively. If l is the least common multiple of m and n, then $l(x \pm y) = lx \pm ly = 0$ and $x \pm y$ has finite order dividing l. It follows that the set of all elements x which satisfy the equation $nx = 0$ forms a subgroup of G, written $G[n]$. By the same token the elements of finite order form a subgroup T, the so-called *torsion-subgroup of* G: clearly G/T is torsion-free. Moreover, elements with order some power of a fixed prime p likewise form a subgroup G_p, the *p-primary component* of G.

Let us consider an arbitrary element x of T and write its order as a product of powers of distinct primes, say $m = p_1^{e_1} \cdots p_k^{e_k}$. Set $m_i = m/p_i^{e_i}$ and observe that the integers $m_1, \ldots, m_k$ have greatest common divisor 1. Consequently it is possible to find integers $l_1, \ldots, l_k$ such that $l_1 m_1 + \cdots + l_k m_k = 1$. Hence $x = (\sum_{i=1}^k l_i m_i)x = \sum_{i=1}^k l_i x_i$ where $x_i = m_i x$. But x_i has order $p_i^{e_i}$ and therefore belongs to G_{p_i}. Consequently T is the sum of all the primary components G_p. Now consideration of orders of elements should convince the reader that $G_p \cap \sum_{q \neq p} G_q = 0$; thus T is in fact the direct sum of the G_p's. These conclusions are now summed up.

4.1.1 (The Primary Decomposition Theorem). *In an abelian group G the torsion-subgroup T is the direct sum of the primary components of G.*

This theorem has the effect of focusing our attention on two classes of abelian groups, torsion-free groups and torsion groups: moreover it reduces the study of the latter to that of abelian p-groups.

Height

An element of g of an abelian group G is said to be *divisible* in G by a positive integer m if $g = mg_1$ for some g_1 in G. If p^h is the largest power of the prime p dividing g, then h is called the *p-height* of g in G: should g be divisible by every power of p, we say that g has *infinite p-height* in G. The notion of height, which is dual to that of order in the sense that $p^m G$ is dual to $G[p^m]$, is especially important in the study of torsion-free groups when order is useless.

An abelian group G is said to be *divisible* if each element is divisible by every positive integer. This is equivalent to saying that each element of G has infinite p-height for all primes p.

Quasicyclic Groups

The divisible group that comes first to mind is probably the additive group of rational numbers $\mathbb{Q}$; this, of course, is torsion-free. Obviously a quotient of a divisible group is divisible, so $\mathbb{Q}/\mathbb{Z}$ is divisible; this is a torsion group since $n(m/n + \mathbb{Z}) = 0_{\mathbb{Q}/\mathbb{Z}}$. By 4.1.1 the group $\mathbb{Q}/\mathbb{Z}$ is the direct sum of its primary components, each of which is also divisible. Now the p-primary component $\bar{P}$ of $\mathbb{Q}/\mathbb{Z}$ consists of all cosets $(m/p^i) + \mathbb{Z}$ and is generated by the $b_i = (1/p^i) + \mathbb{Z}$, $i = 1, 2, \ldots$. These satisfy the relations $pb_1 = 0$ and $pb_{i+1} = b_i$.

Conversely let P be the group with generators $a_1, a_2, a_3, \ldots$ and defining relations

$$pa_1 = 0, \qquad pa_{i+1} = a_i, \qquad \text{and} \qquad a_i + a_j = a_j + a_i.$$

Certainly P is an abelian p-group. Moreover the mapping $a_i \mapsto b_i$ extends to an epimorphism $\varphi: P \to \bar{P}$, by von Dyck's theorem (2.2.1). To see that φ is an isomorphism observe first that each element of P can be written in the form ma_i for suitable integers m and i, in view of the relations $pa_{j+1} = a_j$. Now φ maps ma_i to $mb_i = (m/p^i) + \mathbb{Z}$, which is trivial if and only if p^i divides m; but in this case $ma_i = 0$ because $p^i a_i = 0$.

We have therefore shown that the group P can be realized as the p-component of $\mathbb{Q}/\mathbb{Z}$ and is a divisible abelian p-group. P is called a *Prüfer group of type p^∞*, or a *quasicyclic p-group*. This group appeared in 1.4 as a direct limit of cyclic subgroups of orders $p, p^2, \ldots$.

We shall shortly see that every divisible abelian group is a direct sum of quasicyclic groups and copies of $\mathbb{Q}$.

The Injective Property of Divisible Abelian Groups

An abelian group G is said to be *injective* if, given a monomorphism $\mu: H \to K$ and a homomorphism $\alpha: H \to G$, with H and K abelian groups, one can find a homomorphism $\beta: K \to G$ such that $\alpha = \mu\beta$, in other words such that the diagram

$$\begin{array}{ccc} H & \xrightarrow{\ \mu\ } & K \\ {\scriptstyle \alpha}\downarrow & \swarrow{\scriptstyle \beta} & \\ G & & \end{array}$$

is commutative.

Let us examine what this says. Since μ is monic, $H \simeq \operatorname{Im} \mu \leq K$. Suppose that H is actually a subgroup of K and μ is the inclusion map. Then the assertion of the injective property is that $\alpha: H \to G$ may be extended to a homomorphism $\beta: K \to G$ in the sense that α is the restriction of β to H.

What is the relation between divisibility and injectivity? They are one and the same property.

4.1.2 (Baer†). *An abelian group is injective if and only if it is divisible.*

Proof. (i) Firstly assume that G is injective. Let g be any element of G and m any positive integer: we must prove that m divides g. Now the assignment $m \mapsto g$ determines a homomorphism $\alpha: m\mathbb{Z} \to G$. If ι is the inclusion map, the injective property permits the formation of the commutative diagram

$$\begin{array}{ccc} m\mathbb{Z} & \xrightarrow{\ \iota\ } & \mathbb{Z} \\ {\scriptstyle \alpha}\downarrow & \swarrow{\scriptstyle \beta} & \\ G & & \end{array}$$

with β a homomorphism. Then $g = (m)\alpha = (m)\iota\beta = (m)\beta = m((1)\beta)$, whence m divides g.

(ii) Conversely let G be divisible: to prove that G is injective is harder. Assume that we are given $\mu: H \to K$ and $\alpha: H \to G$, a monomorphism and a homomorphism respectively. Since we can replace H by $\operatorname{Im} \mu$, there is nothing lost in taking μ to be the inclusion map, so that H is a subgroup of K. Our problem is to extend α to K.

† Reinhold Baer (1902–1979).

Let us consider the set **S** of all partial extensions $\gamma: L \to G$ of α. This means that $H \leq L \leq K$ and γ is a homomorphism such that $h\gamma = h\alpha$ for all h in H. We agree to order the set **S** by writing $\gamma \leq \gamma'$ if $\gamma: L \to G$ and $\gamma': L' \to G$ are such that $L \subseteq L'$ and γ' is an extension of γ. We aim to apply Zorn's Lemma to **S** and to this end we consider a chain $\{\gamma_i | i \in I\}$ in **S** with $\gamma_i: L_i \to G$. Put $L = \bigcup_{i \in I} L_i$ and let $\gamma: L \to G$ be defined by $x\gamma = x\gamma_i$ when $x \in L_i$; this is unambiguous since γ_i and γ_j agree where both are defined. Then $\gamma \in \mathbf{S}$ and γ is an upper bound for the chain.

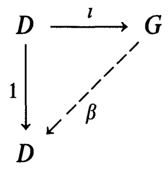
Applying Zorn's Lemma we choose a maximal element $\beta: L \to G$ of **S**. If $L = K$, our task is completed, so we suppose that there exists an element x in $K \backslash L$. If it can be shown that β extends to $L + \langle x \rangle = M$, this will contradict the maximality of L and terminate the proof.

If $L \cap \langle x \rangle = 0$, then $M = L \oplus \langle x \rangle$ and we can extend β to $\beta_1: M \to G$ by simply setting $x\beta_1 = 0$. If $L \cap \langle x \rangle \neq 0$, there is a least positive integer m such that $mx \in L$. Suppose that β maps mx to g in G. Since G is divisible, $g = mg_1$ for some g_1 in G. Now every element of M can be uniquely written in the form $l + tx$ where $l \in L$ and $0 \leq t < m$, by minimality of m. Thus we can define a function $\beta_1: M \to G$ by writing $(l + tx)\beta_1 = l\beta + tg_1$. The reader is invited to perform the routine verification that β_1 is a homomorphism. □

The most important consequence of 4.1.2 is the direct summand property of divisible groups.

4.1.3 (Baer). *If D is a divisible subgroup of an abelian group G, then $G = D \oplus E$ for some subgroup E.*

Proof. Let $\iota: D \to G$ be the inclusion map. By the injective property (4.1.2) there is a homomorphism $\beta: G \to D$ making the diagram



commutative; thus $d\beta = d$ for all d in D. If $g \in G$, then $g\beta \in D$ and thus $g\beta = g\beta^2$. Hence $g - g\beta \in \text{Ker } \beta = E$, say. It follows that $G = D + E$. Finally, if $d \in D \cap E$, then $d = d\beta = 0$. Hence $G = D \oplus E$. □

An abelian group is said to be *reduced* if it has no nontrivial divisible subgroups. The next result reduces our study to that of reduced groups and divisible groups.

4.1.4. *If G is an abelian group, there exists a unique largest divisible subgroup D of G. Moreover $G = D \oplus E$ where E is a reduced group.*

Proof. Define D to be the subgroup generated by all the divisible subgroups of G. One sees at once that D is divisible. By 4.1.3 it is possible to write $G = D \oplus E$. Of course E is reduced. □

The Structure of Divisible Abelian Groups

The following theorem completely describes the class of divisible abelian groups.

4.1.5. *An abelian group G is divisible if and only if it is a direct sum of isomorphic copies of $\mathbb{Q}$ and of quasicyclic groups.*

Proof. We saw that $\mathbb{Q}$ and a group of type p^∞ are divisible. Since a sum of divisible groups is evidently divisible, the sufficiency of the condition follows.

Now assume that G is divisible and let T be its torsion-subgroup. We claim that T is divisible: for if $x \in T$ and $m > 0$, there is certainly an element y in G such that $my = x$, and hence such that $m(y + T) = 0_{G/T}$. But G/T is torsion-free, so $y \in T$ and T is divisible. By 4.1.1 the group T is the direct sum of its primary components, each of which, as an image of T, must be divisible. Moreover 4.1.3 shows T to be a direct summand of G. Consequently, it is enough to prove the theorem in two special cases: G torsion-free and G a p-group.

Suppose first of all that G is torsion-free. Let $g \in G$ and let m be a positive integer; then $g = mg_1$ for some g_1 in G, and in fact for precisely *one* g_1 in G: for $mg_1 = mg_2$ implies that $m(g_1 - g_2) = 0$ and hence that $g_1 = g_2$, because G is torsion-free. Thus it is meaningful to define $(1/m)g$ as this g_1. We now have an action of $\mathbb{Q}$ on G which, it is easy to verify, makes G into a $\mathbb{Q}$-module. But a module over $\mathbb{Q}$ is simply a rational vector space and as such it has a basis. Viewed as an additive abelian group therefore, G is a direct sum of copies of $\mathbb{Q}$.

Now let G be a p-group and write P for $G[p]$. Then P is a module over the field $\mathbb{Z}/p\mathbb{Z}$ by means of the action $x(n + p\mathbb{Z}) = nx$, $(x \in P, n \in \mathbb{Z})$. Hence P is a vector space: let its dimension be $\mathfrak{c}$ (a cardinal number). Now form a direct sum G^* of $\mathfrak{c}$ groups of type p^∞ and write $P^* = G^*[p]$. Then P^* too is a vector space of dimension $\mathfrak{c}$ over $\mathbb{Z}/p\mathbb{Z}$, and there is a monomorphism $\alpha: P^* \to G$ mapping P^* isomorphically onto P. Using the injectivity of G we can extend α to a homomorphism $\beta: G^* \to G$. If Ker β were nonzero, it would have to contain an element of order p and α could not be monic. If Im $\beta \neq G$, the divisible group Im β would be a proper direct summand of G and in that case α could not be surjective. Hence $\beta: G^* \to G$ is an isomorphism and the proof is complete. □

Subgroups of Divisible Groups

The reader will perhaps have noticed that a subgroup of a divisible group need not be divisible—consider $\mathbb{Q}$ for example. In fact the subgroups of divisible groups account for all abelian groups in the sense of the following result.

4.1.6. *Every abelian group is isomorphic with a subgroup of a divisible abelian group.*

Proof. Let F be a free abelian group. It was shown in 2.3.8 that F is a direct sum of infinite cyclic groups; hence F is isomorphic with a subgroup of a direct sum D of copies of $\mathbb{Q}$. Now every abelian group is an image of some such F and hence is isomorphic with a subgroup of a quotient group of D. But a quotient of D, like D itself, is divisible, so we are done. □

EXERCISES 4.1

*1. Prove that a group of type p^∞ has exactly one subgroup of each order p^i and this is cyclic. Show also that every proper subgroup is finite.

2. If G is an infinite abelian group all of whose proper subgroups are finite, then G is of type p^∞ for some prime p.

3. Establish the dual of Exercise 4.1.2. If G is an infinite abelian group all of whose proper quotient groups are finite, then G is infinite cyclic.

4. Prove that an abelian group G is divisible if and only if it has the following property: $G \simeq H \leq K$ always implies that H is a direct summand of K.

5. Describe the structure of the following groups: $\mathbb{R}$, $\mathbb{R}^*$, $\mathbb{C}$, $\mathbb{C}^*$.

6. Let G be an abelian p-group such that $G/G[p]$ is divisible. Prove that G is the direct sum of a divisible group and an elementary abelian p-group.

4.2. Direct Sums of Cyclic and Quasicyclic Groups

The principal theorems of this section describe the structure of finite abelian groups, abelian groups with the maximal condition, and abelian groups with the minimal condition. All these groups possess direct decompositions with cyclic or quasicyclic summands.

Linear Independence and Rank

Let G be an abelian group and let S be a nonempty subset of G. Then S is called *linearly independent*, or simply *independent*, if $0 \notin S$ and, given distinct

elements $s_1, \dots, s_r$ of S and integers $m_1, \dots, m_r$, the relation $m_1 s_1 + \cdots + m_r s_r = 0$ implies that $m_i s_i = 0$ for all i. If S is not independent, it is of course said to be *dependent*. The definition implies at once that the group G is a direct sum of cyclic groups if and only if it is generated by an independent subset: such a subset is called a *basis* of G.

Zorn's Lemma shows that every independent subset of G is contained in a maximal independent subset. Moreover, if we restrict attention to independent subsets consisting of elements of infinite order or of elements of order some power of a fixed prime, we obtain maximal independent subsets consisting of elements of these types.

If p is a prime and G an abelian group, the *p-rank* of G

$$r_p(G)$$

is defined as the cardinality of a maximal independent subset of elements of p-power order. Similarly the *0-rank* or *torsion-free rank*

$$r_0(G)$$

is the cardinality of a maximal independent subset of elements of infinite order. Also important is the *Prüfer rank*, often just called *the rank of* G,

$$r(G) = r_0(G) + \max_p r_p(G).$$

These definitions would be of very little use if they depended on the chosen maximal independent subset. Let us show that this is not so.

4.2.1. *If G is an abelian group, two maximal independent subsets consisting of elements with order a power of the prime p have the same cardinality. The same is true of maximal independent subsets consisting of elements of infinite order. Thus $r_0(G)$, $r_p(G)$, and $r(G)$ depend only on G.*

Proof. Let S be a maximal independent subset of elements of p-power order. If we replace each element of S with order larger than p by a suitable multiple, we obtain an independent subset S_0 consisting of elements of order p such that $|S| = |S_0|$. If $g \in G[p]$, then $S \cup \{g\}$ is dependent and there is a relation $mg + \sum_i m_i s_i = 0$ where $s_i \in S$, m_i, m are integers and $mg \neq 0$. Since $pg = 0$, we have $\sum_i pm_i s_i = 0$ and $pm_i s_i = 0$. Hence $m_i s_i \in \langle S_0 \rangle$ and $g \in \langle S_0 \rangle$. Consequently $G[p] = \langle S_0 \rangle$ and S_0 is a basis of the vector space $G[p]$. Hence $|S| = \dim G[p]$.

Now let S be an independent subset of elements of infinite order. If T is the torsion-subgroup of G, define $\bar{S} = \{s + T | s \in S\}$. In fact $\bar{S}$ is independent in G/T. For if $\sum_i m_i(s_i + T) = 0_{G/T}$ with $s_i \in S$, then $\sum_i m_i s_i \in T$ and $\sum_i m_i n s_i = 0$ for some positive integer n; it follows that $m_i n s_i = 0$ and $m_i = 0$. Let $\bar{U}$ be an independent subset of G/T containing $\bar{S}$, and suppose that $u + T \in \bar{U} \backslash \bar{S}$. Then $\{u\} \cup S$ is independent, which contradicts the maximality of S. Thus $\bar{S}$ is a maximal independent subset of G/T, and clearly $|\bar{S}| = |S|$. Hence we can assume that $T = 0$ and G is torsion-free.

Let $G^* = G \otimes \mathbb{Q}$. Since G is torsion-free, the mapping $g \mapsto g \otimes 1$ is a monomorphism from G to G^* (see Exercise 4.2.8). If $g \in G$, then $S \cup \{g\}$ is dependent and $mg \in \langle S \rangle$ for some $m > 0$. Thus $m(g \otimes 1) \in \langle S^* \rangle$ where $S^* = \{s \otimes 1 \mid s \in S\}$. Hence S^* generates G^* as $\mathbb{Q}$-vector space. Clearly S^* is independent, so it is a $\mathbb{Q}$-basis of G^* and $|S| = |S^*| = \dim G^*$. □

Let us use the concept of rank to show that if an abelian group can be decomposed into a direct sum of cyclic or quasicyclic groups, the summands of the decomposition are essentially unique.

4.2.2. *Suppose that an abelian group G can be expressed in two ways as a direct sum of quasicyclic groups, cyclic groups of prime-power order and infinite cyclic groups. Then the sets of direct summands of each isomorphism type in the two decompositions have the same cardinality.*

Proof. Clearly the cardinality of the set of torsion-free summands in either decomposition equals $r_0 G$. To prove the statement about p-summands we can assume that G is a p-group. Now the cardinality of the set of summands of order p^{n+1} in either decomposition equals that of the factor

$$p^n G \cap G[p] / p^{n+1} G \cap G[p],$$

which depends only on G. Clearly the summands of type p^∞ in either decomposition generate the p-component of the maximal divisible subgroup D of G and they form a set of cardinality $\dim(D[p])$. □

Two points about this result are worth noting. Firstly 4.2.2 is not a consequence of the Krull–Remak–Schmidt theorem—why not? Nor does 4.2.2 guarantee the uniquencess of a direct decomposition into cyclic subgroups; indeed $\mathbb{Z}_6 \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_2$, so there is no uniquencess of this sort.

Free Abelian Groups

By definition a free abelian group is a free group in the variety of abelian groups. It was shown in 2.3.8 that these groups are just direct sums of infinite cyclic groups. Whereas every abelian group is an image of a free abelian group, it is an important theorem that all subgroups of free abelian groups are likewise free abelian.

4.2.3. *If F is a free abelian group on a set X and H is a subgroup of F, then H is free abelian on a set Y where $|Y| \leq |X|$.*

Proof. Let X be well-ordered in some fashion, say as $\{x_\alpha \mid \alpha < \beta\}$ where β is an ordinal number. Define $F_\alpha = \langle x_\gamma \mid \gamma < \alpha \rangle$: then $F_{\alpha+1} = F_\alpha \oplus \langle x_\alpha \rangle$ and

$F_\beta = F$. Writing H_α for $H \cap F_\alpha$, we have from the Second Isomorphism Theorem

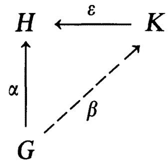
$$H_{\alpha+1}/H_\alpha \simeq (H \cap F_{\alpha+1})F_\alpha/F_\alpha \leq F_{\alpha+1}/F_\alpha \simeq \langle x_\alpha \rangle.$$

Thus, either $H_\alpha = H_{\alpha+1}$ or $H_{\alpha+1}/H_\alpha$ is infinite cyclic. We may therefore write $H_{\alpha+1} = H_\alpha \oplus \langle y_\alpha \rangle$ where y_α may be 0. Clearly H is the direct sum of the $\langle y_\alpha \rangle$'s and H is free on the set $Y = \{y_\alpha \neq 0 \mid \alpha < \beta\}$. □

The Projective Property of Free Abelian Groups

There is a duality between free abelian groups and divisible abelian groups the nature of which is best seen by means of what is known as the projective property.

An abelian group G is said to be *projective* if, given an epimorphism $\varepsilon: K \to H$ and a homomorphism $\alpha: G \to H$, for some abelian groups H and K, there is a homomorphism $\beta: G \to K$ such that $\beta\varepsilon = \alpha$, that is, the following diagram commutes:



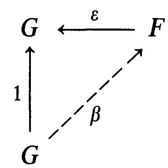
Observe that projectivity is derived from injectivity by reversing all arrows and replacing monomorphisms by epimorphisms. In this sense the two properties are dual.

In 4.1.2 we were able to identify the groups with the injective property. Let us do the same for groups with the projective property.

4.2.4 (MacLane). *An abelian group G is projective if and only if it is free abelian.*

Proof. First suppose that G is free abelian on a subset X. Let $\varepsilon: K \to H$ and $\alpha: G \to H$ be given homomorphisms with ε surjective. Given x in X we can find k_x in K such that $(k_x)\varepsilon = x\alpha$. Define a homomorphism $\beta: G \to K$ by means of $x\beta = k_x$. Then $(x)\beta\varepsilon = (k_x)\varepsilon = x\alpha$ and $\beta\varepsilon = \alpha$. Hence G is projective.

Conversely, let G be projective. By 2.3.7 there is an epimorphism $\varepsilon: F \to G$ with F free abelian. Applying the projective property to the diagram

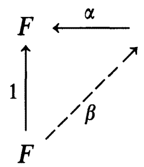


we obtain a homomorphism $\beta: G \to F$ such that $\beta\varepsilon = 1$. Then $\text{Ker}\,\beta = 0$ and $G \simeq \text{Im}\,\beta \leq F$. Now apply 4.2.3 to conclude that G is free abelian. $\square$

Dual to 4.1.6 is the already proven fact that every abelian group is an image of a free abelian group. Dual to the direct summand property of divisible abelian groups is the following.

4.2.5. *If G is an abelian group and H is a subgroup such that G/H is free abelian, then $G = H \oplus K$ for some subgroup K.*

Proof. Let $F = G/H$ and denote the canonical homomorphism from G to F by α. Then, F being projective, there is a commutative diagram



with β a homomorphism: thus $\beta\alpha = 1$. If $g \in G$, we have $(g - (g)\alpha\beta)\alpha = (g)\alpha - (g)\alpha = 0$, so $g \in \text{Ker}\,\alpha + \text{Im}\,\beta$; hence $G = \text{Ker}\,\alpha + \text{Im}\,\beta$. Moreover $\beta\alpha = 1$ implies that $\text{Ker}\,\alpha \cap \text{Im}\,\beta = 0$. Hence $G = \text{Ker}\,\alpha \oplus \text{Im}\,\beta$: of course $\text{Ker}\,\alpha = H$. $\square$

Structure of Finite Abelian Groups

The following result, which was the first significant structure theorem to be obtained in the theory of groups, classifies all finite abelian groups.

4.2.6 (Frobenius–Stickelberger†). *An abelian group G is finite if and only if it is a direct sum of finitely many cyclic groups with prime-power orders.*

The proof is based on a lemma.

4.2.7. *Let G be an abelian p-group whose elements have bounded orders and let g be an element of maximal order in G. Then $\langle g \rangle$ is a direct summand of G.*

Proof. By Zorn's Lemma there is a subgroup M which is maximal subject to $M \cap \langle g \rangle = 0$. If $G = M + \langle g \rangle$, then $G = M \oplus \langle g \rangle$ and the proof is complete. Assume, therefore, that $G \neq M + \langle g \rangle$ and let x be an element of minimal order in $G \backslash (M + \langle g \rangle)$. By choice of x we have $px \in M + \langle g \rangle$ and thus $px = y + lg$ where $y \in M$. Since g has maximal order in G—let us say

† Ludwig Stickelberger (1850–1936).

p^n—we have $0 = p^n x = p^{n-1}y + p^{n-1}lg$ and $p^{n-1}lg \in M \cap \langle g \rangle = 0$. Consequently, p^n divides $p^{n-1}l$ and p divides l. Now write $l = pj$, so that $p(x - jg) = y \in M$, while $x - jg \notin M$ since $x \notin M + \langle g \rangle$. From the maximality of M we know that $\langle x - jg, M \rangle \cap \langle g \rangle \neq 0$, which implies that there exist integers k and u and an element y' of M such that $0 \neq kg = u(x - jg) + y'$. Hence $ux \in M + \langle g \rangle$. Suppose that $p|u$; then, since $p(x - jg) \in M$, it follows that $u(x - jg) \in M$ and thus $kg = 0$. Hence $(p, u) = 1$. However $px \in M + \langle g \rangle$, so $x \in M + \langle g \rangle$, a contradiction. □

***Proof of* 4.2.6.** This is now easy. Suppose that G is finite. By 4.1.1 we can assume that G is a nontrivial p-group. If g is an element of maximum order in G, then $G = G_1 \oplus \langle g \rangle$ by 4.2.7. But $|G_1| < |G|$, so we can apply induction on the group order to G_1 and obtain the result. The converse is obvious. □

Structure of Finitely Generated Abelian Groups

Any group, commutative or noncommutative, with the maximal condition on subgroups is finitely generated (3.1.6): for abelian groups the converse is true.

4.2.8. *An abelian group G satisfies the maximal condition if it is finitely generated.*

Proof. Let G be generated by $g_1, \dots, g_n$. If $n = 1$, then G is cyclic and Exercise 1.3.6 shows that every nontrivial subgroup has finite index; in this case G clearly has max. If $n > 1$, the subgroup $H = \langle g_1, \dots, g_{n-1} \rangle$ has max by induction on n, as does the cyclic group G/H. Finally G has max by 3.1.7. □

We note another result of an elementary character.

4.2.9. *A finitely generated abelian group G is finite if it is a torsion group.*

Proof. If $G = \langle g_1, \dots, g_n \rangle$ and $G_i = \langle g_i \rangle$, then G is the sum of the finite groups $G_1, \dots, G_n$. Hence G is finite. □

Next we shall prove an important theorem that completely classifies finitely generated abelian groups.

4.2.10. *An abelian group G is finitely generated if and only if it is a direct sum of finitely many cyclic groups of infinite or prime-power orders.*

Proof. Let G be finitely generated. First of all suppose that G is torsion-free and let $G = \langle g_1, \dots, g_n \rangle$: we can of course assume that $n > 1$. Define H to

be the set of all x in G such that $nx \in \langle g_1 \rangle$ for some positive integer n. We speedily verify H to be a subgroup: moreover if $m \neq 0$ and $mx \in H$, then $nmx \in \langle g_1 \rangle$ for some $n > 0$, which shows that $x \in H$ and G/H is torsion-free. Since G/H can be generated by the $n - 1$ elements $g_2 + H, \dots, g_n + H$, induction on n shows G/H to be a direct sum of infinite cyclic groups; thus G/H is free abelian. Applying 4.2.5, we can find a subgroup K such that $G = H \oplus K$ where K is free abelian. Now $H/\langle g_1 \rangle$ is certainly a torsion group. Since G has max (4.2.8), we can say that H is finitely generated and it then follows from 4.2.9 that $H/\langle g_1 \rangle$ is finite. Consequently there is a positive integer m such that $mH \leq \langle g_1 \rangle$ and the mapping $x \mapsto mx$ is a monomorphism $x \mapsto mx$ from H into $\langle g_1 \rangle$. Hence H is infinite cyclic and $G = H \oplus K$ is free abelian.

In the general case let T be the torsion-subgroup of G. By the first part of the proof G/T is free abelian and 4.2.5 shows that $G = F \oplus T$ where F is free abelian of finite rank. Now T is a finitely generated torsion group, so it is finite by 4.2.9 and we may apply 4.2.6 to T to obtain the result. □

By 4.2.10 a finitely generated abelian group may be decomposed in a direct sum of l_0 infinite cyclic groups and $l_{p,i}$ cyclic groups of order p^i (where p is a prime and $i = 1, 2, \dots$); moreover the nonnegative integers, l_0, $l_{p,i}$ constitute a set of invariants of G which determine the group to within isomorphism. Perfect classification theorems of this type are, unfortunately, a rarity in group theory.

Structure of Abelian Groups with the Minimal Condition

Noting that 4.2.10 describes the abelian groups with max, we turn to abelian groups with min.

4.2.11 (Kuroš). *An abelian group G satisfies the minimal condition if and only if it is a direct sum of finitely many quasicyclic groups and cyclic groups of prime-power order.*

Proof. Assume that G has min. Keeping in mind that any group with min is a torsion group (Exercise 3.1.7), we write G as the direct sum of its primary components, and we observe that all but a finite number of these components are trivial. Thus we may suppose that G is a p-group. Also, in view of 4.1.4 and 4.1.5, we can take G to be a reduced group; the problem before us now is to show that G is finite. Let us suppose that G is infinite. Then on the basis of the minimal condition we can find a minimal infinite subgroup H of G. If $H = pH$, then H is divisible and hence $H = 0$ by reducibility of G. Consequently, $pH < H$ and pH is finite, by minimality of H. Now $H/H[p] \simeq pH$ by the First Isomorphism Theorem. Hence $H/H[p]$ is finite and $H[p]$ must be infinite. But $H[p]$ is a direct sum of groups of order p and min forces it to be finite.

Conversely a quasicyclic group has min because every proper subgroup is finite (Exercise 4.1.1). Application of 3.1.7 now shows that a direct sum of the prescribed type has min. □

The decomposition of G obtained in 4.2.11 is unique in the sense of 4.2.2: thus abelian groups with min also have a simple set of invariants.

Exercises 4.2

1. If G is a free abelian group on a set with n elements, prove that G cannot be generated by fewer than n elements.
2. If G is an abelian group, show that $r(G)$ is finite if and only if $\max\{d(H)\}$ is finite where H ranges over the finitely generated subgroups of G. Prove that in this case case $r(G) = \max\{d(H)\}$. [*Note*: $d(H)$ is the minimum number of generators of H.]

*3. If G is a finitely generated abelian group, show that $d(G) = r(G)$. Also $d(G) = r_0(G)$ if and only if G is torsion-free.

*4. If A and B are finitely generated abelian groups and B is torsion-free, show that $d(A \oplus B) = d(A) + d(B)$.

5. Prove that an abelian group has rank ≤ 1 if and only if it is isomorphic with a subgroup of $\mathbb{Q}$ or $\mathbb{Q}/\mathbb{Z}$.
6. A group is torsion-free abelian of rank $\leq r$ if and only if it is isomorphic with a subgroup of a rational vector space of dimension r.

*7. If H is a subgroup of an abelian group G, prove that the following are valid:
(i) $r_0(H) + r_0(G/H) = r_0(G)$;
(ii) $r_p(H) + r_p(G/H) \geq r_p(G)$, with inequality in general.

*8. (Dieudonné).Let $\mu: A \to B$ be a monomorphism of abelian groups and let G be a torsion-free abelian group. Prove that $\mu_*: A \otimes_{\mathbb{Z}} G \to B \otimes_{\mathbb{Z}} G$ is a monomorphism where $(a \otimes g)\mu_* = (a\mu) \otimes g$ [*Hint*: Reduce first to the case where G is finitely generated and then to the case $G = \mathbb{Z}$.]

*9. An abelian group G is free if and only if it has the following property: if K is a subgroup of an abelian group H and $H/K \simeq G$, then K is a direct summand of H.

10. If G is finitely generated abelian group, every surjective endomorphism of G is an automorphism.
11. If G is an abelian group with min, every injective endomorphism of G is an automorphism.
12. How many isomorphism types are there of abelian groups of order p^n?
13. If G is a finite abelian group whose order is divisible by m, prove that G has a subgroup and a quotient group of order m.
14. Let G and H be two finite abelian groups. If for every integer m they contain the same number of elements of order m, then $G \simeq H$.

*15. Prove that a finitely generated abelian group is residually finite.

4.3. Pure Subgroups and p-Groups

A very important notion in the theory of abelian groups is that of purity. A subgroup H of an abelian group G is called *pure* if

$$nG \cap H = nH$$

for all integers $n \geq 0$; in words, H is pure if every element of H that is divisible by n in G is divisible by n in H. If G is a p-group, it is easy to see that H is pure in G if and only if $p^m G \cap H = p^m H$ for all positive integers m.

For example, if H is a direct summand of G and $G = H \oplus K$, then $nG \cap H = (nH + nK) \cap H = nH$ by the modular law. Hence every *direct summand of G is pure*. It may be helpful for the reader to think of a pure subgroup as a generalization of a direct summand.

If H is a subgroup of G such that G/H is torsion-free, then clearly H is pure: in particular the torsion-subgroup of G is pure. This is a source of pure subgroups that are usually not direct summands.

If $H \leq K \leq G$ and K is pure in G, then obviously K/H is pure in G/H. If H is pure in G, the converse of this statement is true.

4.3.1. *Let $H \leq K \leq G$ where G is an abelian group. If H is pure in G and K/H is pure in G/H, then K is pure in G.*

Proof. Let $k \in nG \cap K$ and write $k = ng$ where $g \in G$. Then $k + H = n(g + H)$, whence, by purity of K/H, we have $k + H = n(k' + H)$ for some k' in K. Thus $h = k - nk' \in H$. Since $h = ng - nk' = n(g - k')$, the purity of H in G yields $h = nh'$ with h' in H; therefore $k = nh' + nk' = n(h' + k') \in nK$. This proves the result. □

In speaking of the *height* of an element in an abelian p-group G we shall always mean the p-height. The elements of infinite height in G are precisely the elements of the subgroup $\bigcap_{n=1,2,\ldots} p^n G$.

4.3.2. *Let G be an abelian p-group. If every element of order p has infinite height, then G is divisible.*

Proof. If G is not divisible, there exists an element g of smallest order which is not divisible by p. Let $|g| = p^m$; by hypothesis $m > 1$. Now $p^{m-1}g$ has order p and thus has infinite height. Hence we can certainly write $p^{m-1}g = p^m g_1$ for some g_1 in G. It follows that $p^{m-1}(g - pg_1) = 0$ and $g_2 = g - pg_1$ has order at most p^{m-1}. By minimality of m it is possible to write $g_2 = pg_3$ for some g_3 in G. Therefore $g = g_2 + pg_1 = p(g_3 + g_1)$, in contradiction to our choice of g. □

This result may be used to establish the existence of pure cyclic subgroups in groups which are not divisible.

4.3.3. *Let G be an abelian p-group which is not divisible. Then G has a nontrivial pure cyclic subgroup.*

Proof. By 4.3.2 there is an element g of $G[p]$ with finite height, say m. Then $g = p^m h$ with $h \in G$, and $g \notin p^{m+1}G$. We shall prove that $\langle h \rangle$ is pure in G. Since G is a p-group, it is sufficient to establish the equality $p^i G \cap \langle h \rangle = p^i \langle h \rangle$ for all $i > 0$. Suppose that i is the smallest positive integer for which this fails to hold.

In the first place $p^i G \cap \langle h \rangle$ is contained in $p^{i-1} G \cap \langle h \rangle$ and hence in $p^{i-1}\langle h \rangle$. If $m < i - 1$, then $|h| = p^{m+1} \leq p^{i-1}$ and $p^{i-1}\langle h \rangle = 0$; in this case $p^i G \cap \langle h \rangle = 0 = p^i \langle h \rangle$. It follows that $m \geq i - 1$. Then $g = p^{m-i+1}(p^{i-1}h)$, whence $p^{i-1}h \notin p^i G$. This implies that $p^i G \cap \langle h \rangle$ must be a proper subgroup of $p^{i-1}\langle h \rangle$. Hence $p^i G \cap \langle h \rangle \leq p^i \langle h \rangle$, a contradiction. □

Basic Subgroups

Let G be an abelian torsion group. A subgroup B is called a *basic subgroup* if it is pure in G, it is a direct sum of cyclic groups, and G/B is divisible. Such subgroups play an important role in the theory of abelian p-groups. Our first task is to prove that they are always present.

4.3.4 (Kulikov). *Every abelian torsion group G has a basic subgroup.*

Proof. If B_p is a basic subgroup of the p-primary component of G, it is easy to see that $B = \text{Dr}_p\, B_p$ is basic in G. Therefore we may restrict ourselves to the case where G is a p-group. In addition, should G be divisible, 0 will qualify as a basic subgroup. Hence we may suppose that G is not divisible.

Let us call a nonempty subset X *pure-independent* if it is independent and $\langle X \rangle$ is pure. On the basis of 4.3.3 we may be certain that pure-independent subsets exist. Clearly the union of a chain of pure-independent subsets is pure-independent. Thus Zorn's Lemma may be invoked to provide us with a maximal pure-independent subset X. Let $B = \langle X \rangle$: if we can establish that G/B is divisible, it will follow that B is basic. Assume therefore that this is not the case.

By 4.3.3 the group G/B has a nontrivial pure cyclic subgroup $\langle g + B \rangle$. If $p^d g \in B$, then $p^d g \in p^d G \cap B = p^d B$ by purity of B. Hence $p^d g = p^d b$ and $p^d(g - b) = 0$ for some b in B. Since $(g - b) + B = g + B$, it follows that $g' = g - b$ and $g' + B$ have the same order. Now put $Y = X \cup \{g'\}$. If Y were dependent, there would exist a positive integer m such that $0 \neq mg' \in B$: but this conflicts with the fact that the orders of g' and $g' + B$ are equal. Finally B is pure in G and $\langle g' + B \rangle$ is pure in G/B, whence $\langle g', B \rangle = \langle Y \rangle$ is pure in G by 4.3.1. However we have shown that Y is pure-independent, so X is not maximal, our final contradiction. □

Structure of Bounded Abelian Groups

An additively written group is called *bounded* if its elements have boundedly finite orders: of course multiplicative groups with this property are said to have finite exponent but this term is less appropriate in the context of additive groups.

The mere existence of basic subgroups is enough to settle the structure of bounded abelian groups.

4.3.5 (Prüfer, Baer). *An abelian group G is bounded if and only if it is a direct sum of cyclic groups with boundedly finite orders.*

Proof. Let G be bounded and let B be a basic subgroup. Then G/B is both divisible and bounded. But this can only mean that $G = B$, a direct sum of cyclic groups. The converse is clear. □

In general an abelian torsion group has many basic subgroups, but it is a remarkable fact that they are all isomorphic.

4.3.6 (Kulikov, Fuchs). *If G is an abelian torsion group, then all basic subgroups of G are isomorphic.*

Proof. As usual we may assume that G is a p-group. Let B be a basic subgroup of G. Then $G = p^nG + B$ for all $n > 0$, by divisibility of G/B. Also $p^nG \cap B = p^nB$ by purity of B and thus $G/p^nG \simeq B/p^nB$. Now if $k \leq n$, the set of cyclic direct summands of B with order p^k has cardinality equal to that of the set of corresponding summands in B/p^nB and hence in some cyclic direct decomposition of G/p^nG; by 4.2.2 this depends only on G. Hence any two basic subgroups are isomorphic. □

An Example

The following example of a basic subgroup is fundamental in the theory of uncountable abelian p-groups.

Let p be a prime and let H be the cartesian sum of cyclic groups $G_1, G_2, \dots$ of orders $p, p^2, p^3, \dots$. Of course H is an abelian group and its torsion-subgroup G consists of all sequences $(x_2, x_2, \dots)$ where $x_i \in G_i$ and the orders $|x_i|$ are bounded. Also G is a p-group. The direct sum B of the G_i, consisting of all *restricted* sequences $(x_1, x_2, \dots)$ with $x_i = 0$ for almost all i, is plainly a subgroup of G.

4.3.7. *B is a basic subgroup of G.*

Proof. Naturally B is a direct sum of cyclic groups. If $x \in p^m G \cap B$, then $x = p^m(x_1, x_2, \dots) = (y_1, \dots, y_k, 0, 0, \dots)$, for some x_i, y_i in G_i and $k \geq 0$. Hence $y_i = p^m x_i$ and $x = (p^m x_1, \dots, p^m x_k, 0, \dots) = p^m(x_1, x_2, \dots, x_k, 0, \dots) \in p^m B$. Thus B is pure in G. Next let $x = (x_1, x_2, \dots)$ in G have order p^m; then $p^m x_i = 0$ and if $i > m$, we have $x_i \in pG_i$ since $|G_i| = p^i$. Hence $x \in B + pG$ and $G/B = p(G/B)$, which implies that G/B is divisible. □

The group G is an example of a *torsion-complete p-group*, the torsion-subgroup of a cartesian sum of groups $B_1, B_2, \dots$ where B_n is a direct sum of cyclic groups of order p^n. It is a fact that every abelian p-group without nonzero elements of infinite height is isomorphic with a pure subgroup of a torsion-complete p-group (see Exercise 4.3.11).

We mention in passing an important theorem of Szele†: *a basic subgroup of an abelian torsion group is an endomorphic image*: for a proof see [b24].

Pure Bounded Subgroups

It has been remarked that a pure subgroup is a generalization of a direct summand. It is an important fact that for bounded subgroups these concepts are identical.

4.3.8. *A pure bounded subgroup H of an abelian group G is a direct summand.*

Proof. Suppose that $nH = 0$. Let $K = H + nG$ and consider the group $\bar{G} = G/K$. We deduce from 4.3.5 that $\bar{G}$ is a direct sum of cyclic groups, say $\langle x_\lambda + K \rangle$, $\lambda \in \Lambda$. If $x_\lambda + K$ has order n_λ, then $n_\lambda x_\lambda = h_\lambda + ng_\lambda$ where $h_\lambda \in H$ and $g_\lambda \in G$. Now n_λ divides n; hence $h_\lambda = n_\lambda(x_\lambda - (n/n_\lambda)g_\lambda) \in n_\lambda G \cap H = n_\lambda H$, by purity of H. It is therefore possible to write $h_\lambda = n_\lambda h'_\lambda$ with h'_λ in H. Setting $y_\lambda = x_\lambda - h'_\lambda$, we have $n_\lambda y_\lambda = n_\lambda x_\lambda - h_\lambda = ng_\lambda$. Also $y_\lambda + K = x_\lambda + K$.

Define L to be the subgroup generated by nG and the y_λ, $\lambda \in \Delta$. Our aim is to prove that $G = H \oplus L$. If $x = \sum_\lambda m_\lambda y_\lambda + ng \in H$, then $\sum_\lambda m_\lambda(x_\lambda + K) = \sum_\lambda m_\lambda(y_\lambda + K) = 0_{\bar{G}}$, which implies that n_λ divides m_λ by independence of the $x_\lambda + K$. But we saw that $n_\lambda y_\lambda = ng_\lambda$; thus $x = \sum_\lambda m_\lambda y_\lambda + ng \in nG \cap H = nH = 0$. Hence $H \cap L = 0$.

Finally, if $g \in G$ and $g + K = \sum_\lambda l_\lambda(y_\lambda + K)$, one has $g - \sum_\lambda l_\lambda y_\lambda \in K$ and thus $g - \sum_\lambda l_\lambda y_\lambda = h + ng_1$ where $h \in H$, $g_1 \in G$. Therefore

$$g = h + ng_1 + \sum_\lambda l_\lambda y_\lambda,$$

which belongs to $H + L$. Hence $G = H \oplus L$. □

An important application of 4.3.8 is to the question: When is the torsion-subgroup a direct summand?

† Tibor Szele (1918–1955).

4.3.9. *Let T be the torsion-subgroup of an abelian group G. If T is the direct sum of a divisible group and a bounded group, then T is a direct summand of G.*

This follows easily from 4.1.3 and 4.3.8. Let us pause to show that the torsion-subgroup is not always a direct summand.

4.3.10. *If C is the cartesian sum of cyclic groups of orders $p, p^2, p^3, \ldots$, the torsion-subgroup T is not a direct summand of C.*

Proof. Let $C = \mathrm{Cr}_{i=1,2,\ldots} \langle x_i \rangle$ where $|x_i| = p^i$. Denote by y the element of C whose nonzero components are px_2, p^2x_4, p^4x_8 etc. Then $y \notin T$ and $y \in p^nC + T$ for all n. Therefore $y + T$ is a nonzero element of infinite p-height in C/T. Since C has no such elements, T cannot be a direct summand of C. □

A second important application of 4.3.8 pertains to the decomposability of abelian groups.

4.3.11. *If G is an abelian group which is not torsion-free, it has a nontrivial direct summand which is either cyclic or quasicyclic.*

Proof. Let T be the torsion-subgroup of G. If T is divisible, it is a direct summand and G has a quasicyclic direct summand. If T is not divisible, it has a nontrivial pure cyclic subgroup by 4.3.3: applying 4.3.8 we conclude that this is a direct summand of G since it is clearly pure in G. □

This has the immediate effect of determining all indecomposable abelian torsion groups.

4.3.12. *An indecomposable abelian group which is not torsion-free is either a cyclic p-group or a quasicyclic group.*

On the basis of 4.3.11 we can also describe the structure of abelian p-groups which have finite p-rank.

4.3.13. *An abelian p-group G has finite p-rank if and only if it is a direct sum of finitely many cyclic and quasicyclic groups.*

Proof. If $G \neq 0$ and $r_p(G) < \infty$, then G has by 4.3.11 a decomposition $G = G_1 \oplus G_2$ where G_1 is either nontrivial cyclic or quasicyclic. Since $r_p(G) = r_p(G_2) + 1$, we can apply induction on the rank to G_2 and obtain the result required. □

On the basis of 4.3.13 and 4.2.11 we conclude that *for an abelian p-group, to have finite rank is equivalent to the minimal condition.*

Direct Sums of Cyclic p-Groups—Kulikov's Criterion

When is an abelian p-group G a direct sum of cyclic groups? It is not hard to find a necessary condition: G should have no nonzero elements of infinite height because $\bigcap_{n=1,2,\ldots} p^n D = 0$ for any direct sum D of cyclic p-groups.

However this condition by itself does not guarantee that G is a direct sum of cyclic groups. Indeed in 4.3.7 we saw an uncountable abelian p-group G without nonzero elements of infinite height which has a countable basic subgroup B. Such a group could not be a direct sum of cyclic groups: otherwise G would itself be basic and thus $G \simeq B$ by 4.3.6.

Kulikov has shown how to strengthen the condition to make it sufficient.

4.3.14 (Kulikov). *An abelian p-group G is a direct sum of cyclic groups if and only if there is an ascending chain of subgroups $G_1 \leq G_2 \leq \cdots \leq G_n \leq \cdots$ whose union is G such that the height of a nonzero element of G_n cannot exceed some positive integer $k(n)$.*

Proof. If G is a direct sum of cyclic groups, define G_n to be the subgroup generated by all summands of order at most p^n. Clearly no nonzero element of G_n can have height greater than $n - 1$. Hence the G_n's form a chain of the type in question.

Conversely let us assume that G has a chain $\{G_n\}$ with the properties specified. Now there is nothing to be lost in taking $k(n)$ to be $n - 1$: for we may add a finite number of 0's at the beginning of the chain, repeat any G_n a finite number of times and relabel the resulting chain. Our chain will now have the convenient property $p^n G \cap G_n = 0$ for $n = 1, 2, \ldots$.

Consider the set **S** of all chains $\{H_n\}$ such that $G_n \leq H_n$ and $p^n G \cap H_n = 0$ for all n. Let **S** be partially ordered according to rule $\{H_n\} \leq \{K_n\}$ if and only if $H_n \leq K_n$ for all n. We easily verify that Zorn's Lemma is applicable and we use this to select a maximal element of **S**, say $\{H_n\}$.

Choose a basis S_n for the group $p^{n-1}G \cap H_n[p]$. Since $p^n G \cap H_n[p] = 0$, the sets $S_1, S_2, \ldots$ are disjoint, and also their union S is independent. If $s \in S$, write $s = p^{h(s)}g(s)$ where $h(s)$ is the height of s and $g(s) \in G$. Now consider the set $\{g(s) | s \in S\}$. Suppose that this is dependent and $\sum_s m_s g(s) = 0$ where not every $m_s g(s)$ is 0. There is a term in this sum with maximal order, say $m_{s'} g(s')$ with order p^d. Since S is independent, $d > 1$. But $\sum_s m_s p^{d-1} g(s) = 0$ and $m_s p^{d-1} g(s) \in \langle s \rangle$: hence $m_s p^{d-1} g(s) = 0$ for all s and $|m_{s'} g(s')| < p^d$. By this contradiction the set of all $g(s)$ is independent. We shall complete the proof by showing that $G = T$ where $T = \langle g(s) | s \in S \rangle$.

As a first step let us prove that $G[p] \leq T$. Should this be false, there is a least r for which $H_r[p] \nleq T$ since $G_r[p] \leq H_r[p]$. Moreover $r > 1$ because S_1 generates $H_1[p]$. Choose g in $H_r[p] \backslash T$; then $g \notin H_{r-1}$ by minimality of r. Now $p^{r-1}G \cap \langle g, H_{r-1} \rangle \neq 0$; otherwise we could replace H_{r-1} by $\langle g, H_{r-1} \rangle$, thereby contradicting the maximality of the chain $\{H_n\}$ in **S**. Consequently $\langle g \rangle \cap (p^{r-1}G + H_{r-1}) \neq 0$; since $|g| = p$, this means that $g \in p^{r-1}G + H_{r-1}$.

We can now write $g = g_1 + h$ where $g_1 \in p^{r-1}G$ and $h \in H_{r-1}$. Then $g_1 = g - h \in p^{r-1}G \cap H_r$, so $pg_1 \in p^rG \cap H_r = 0$, which shows that

$$g_1 \in p^{r-1}G \cap H_r[p] = \langle S_r \rangle \leq T.$$

Also $ph = p(g - g_1) = 0$ and thus $h \in H_{r-1}[p]$. Minimality of r yields $h \in T$ and $g \in T$, a contradiction.

For the final step we suppose that g is an element of minimal order in $G \backslash T$. By the previous paragraph $|g| = p^{n+1}$ for some $n > 0$ and $p^n g \in T[p]$; thus we can write $p^n g = m_1 s_1 + \cdots + m_k s_k$ with s_i in S since S generates $T[p]$. Let these s_i be so ordered that $s_1, \ldots, s_j$ belong to $S_{n+1} \cup S_{n+2} \cup \cdots$ and $s_{j+1}, \ldots, s_k$ belong to $S_1 \cup \cdots \cup S_n$: here j satisfies $0 \leq j \leq k$. If $i \leq j$, then $m_i s_i = p^n a_i$ where $a_i \in \langle g(s_i) \rangle \leq T$. Hence

$$p^n(g - a_1 - \cdots - a_j) = m_{j+1}s_{j+1} + \cdots + m_k s_k.$$

But $s_{j+1}, \ldots, s_k$ belong to $H_n[p]$ and this intersects p^nG in 0. Therefore $p^n(g - a_1 - \cdots - a_j) = 0$ and $g - a_1 - \cdots - a_j \in T$ by minimality of $|g|$. Finally $g \in T$ because $a_i \in T$. □

Kulikov's criterion has several interesting applications.

4.3.15 (Prüfer). *A countable abelian p-group G is a direct sum of cyclic groups if and only if it contains no nontrivial elements of infinite height.*

Proof. Only the sufficiency of the condition is in question; assume that G has no nonzero elements of infinite height. Since G is countable, its elements may be written g_n, $n = 1, 2, \ldots$. Then $G_n = \langle g_1, \ldots, g_n \rangle$ is finite and $\{G_n\}$ is a chain of subgroups with union equal to G. Since G_n is finite, its non zero elements have boundedly finite heights. Now 4.3.14 gives the result at once. □

It is important to realize that a reduced countable abelian p-group may have nonzero elements of infinite height. An example is the group with generators $x_1, x_2, \ldots$ and relations

$$p^i x_{i+1} = x_1, \qquad px_1 = 0, \qquad x_i + x_j = x_j + x_i$$

(see Exercise 4.3.7).

Subgroups of a Direct Sum of Cyclic Groups

4.3.16 (Kulikov). *If G is a direct sum of cyclic groups, every subgroup of G is likewise a direct sum of cyclic groups.*

Proof. Let $H \leq G$. Suppose first that G is a p-group. By 4.3.14 there is an ascending chain of subgroups $\{G_n\}$ such that $G = \bigcup_n G_n$ and nonzero ele-

ments of G_n have boundedly finite heights. Put $H_n = H \cap G_n$: then $\{H_n\}$ is a chain in H with the same properties as $\{G_n\}$. Hence H is a direct sum of cyclic groups by 4.3.14 again.

In the general case denote the torsion-subgroup of G by T and let G_p be the p-primary component of G. Clearly G/T is a direct sum of infinite cyclic groups, that is, it is free abelian. By 4.2.3 the group $H/H \cap T$ is free abelian. Applying 4.2.5 we write $H = (H \cap T) \oplus K$ where K is free abelian. Finally T is the direct sum of the G_p's, and $H \cap T$ is clearly the direct sum of the $H \cap G_p$'s. But G_p is the direct sum of those summands of G that are p-groups. Hence $H \cap G_p$ is a direct sum of cyclic groups by the first paragraph. The theorem now follows. □

It would be a pity to quit the theory of abelian p-groups without at least mentioning *Ulm's theorem.* This remarkable result does no less than characterize countable reduced abelian p-groups in terms of the cardinalities of certain factors, the so-called *Ulm–Kaplansky invariants.* Two groups are isomorphic precisely when they have identical invariants. Space forbids our presenting this theory here, but the accounts in [b37] and [b25] are warmly recommended to the interested reader.

EXERCISES 4.3

1. If H is pure in K and K is pure in G, then H is pure in G.
2. In a torsion-free abelian group the intersection of a family of pure subgroups is pure. However in a finite abelian group this need not be true.
3. The pure subgroups of a divisible abelian group are just the direct summands.
4. An abelian p-group is divisible if and only if it contains no nontrivial pure cyclic subgroups.

*5. An abelian p-group has finitely many elements of each order if and only if satisfies min. Use this to characterize abelian groups which have only finitely many elements of each order (including ∞).

6. Every abelian p-group is an image of some direct sum of cyclic p-groups.
7. Let G be generated by $x_1, x_2, \dots$ subject to defining relations $px_1 = 0$, $p^i x_{i+1} = x_1$ and $x_i + x_j = x_j + x_i$. Prove that G is a countable reduced abelian p-group containing a nonzero element of infinite height.
8. An abelian p-group has a bounded basic subgroup if and only if it is the direct sum of a divisible group and a bounded group.

*9. Let G be an abelian group such that $r_p(G) < \infty$ if $p = 0$ or a prime.
   (a) If $H \leq G$, show that $r_p(G/H) \leq r_0(G) + r_p(G)$ for all $p > 0$.
   (b) Prove that G/nG is finite for all $n > 0$.

10. If G is an abelian group such that Aut G is finite, prove that G has finite torsion-subgroup. If End G is finite, prove that G is finite.

11. Let G be an abelian p-group with no nontrivial elements of infinite height. Let B be basic in G and write $B = B_1 \oplus B_2 \oplus \cdots$ where B_i is a direct sum of cyclic groups of order p^i. Define C_n to be the subgroup generated by $p^n G$ and B_{n+1}, $B_{n+2}, \ldots$.
    (a) If $g \in G$, prove that there exist elements $b_i \in B_i$ such that
    $$g \equiv b_1 + \cdots + b_n \mod C_n \qquad \text{for all} \quad n \geq 1.$$
    (b) Prove that the mapping $\theta: g \mapsto (b_1, b_2, \ldots)$ is a well-defined monomorphism from G to the torsion-subgroup $\bar{B}$ of $\mathrm{Cr}_{i=1,2,\ldots} B_i$.
    (c) Show that G^θ is pure in $\bar{B}$.
12. If G and B are as in Exercise 4.3.11, prove that $|G| \leq |B|^{\aleph_0}$.
13. Let $G = \langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \cdots$ where $|x_i| = p^{n_i}$ and $n_1 < n_2 < \cdots$. Let B be the subgroup generated by all $\bar{x}_i = x_i - p^{n_{i+1} - n_i} x_{i+1}$. Prove that B is basic in G and $x_1 \notin B$, so $B \neq G$.
14. (Kulikov) Prove that an abelian torsion group has a unique basic subgroup if and only if it is divisible or bounded. [*Hint*: Let B be the unique basic subgroup of the p-group G. Write $B = \langle x \rangle \oplus B_1$ and show that $G = \langle x \rangle \oplus G_1$ for some G_1. If $a \in G_1$ and $|a| \leq |x|$, prove that the assignments $x \mapsto xa$ and $g_1 \mapsto g_1$, $(g_1 \in G_1)$, determine an automorphism of G. Deduce that $a \in B$.]
15. (V. Walter). Prove that an abelian group G has no quasicyclic quotients if and only if there is a finitely generated subgroup H such that G/H is a direct sum of bounded p-groups for various primes p. [*Hint*: Assume that G has no quasicyclic quotients and show that G cannot have a free abelian subgroup with infinite rank. Reduce to the case where G is a torsion group and apply 4.3.4].
16. Let A and B be abelian torsion groups. Prove that $A \otimes_{\mathbb{Z}} B$ is a direct sum of finite cyclic groups. [*Hint*: Use basic subgroups].

4.4. Torsion-Free Groups

Torsion-free abelian groups are much harder to deal with than abelian p-groups and, except in the case of groups of rank 1, no really satisfactory classification exists.† Since a torsion-free abelian group can be embedded in a torsion-free divisible abelian group (Exercise 4.2.6), that is, in a rational vector space, in treating torsion-free abelian groups we are really working with additive subgroups of rational vector spaces.

Height and Type

The concept of height provides an important way of distinguishing between elements in torsion-free abelian groups. In the ensuing discussion we shall suppose that $p_1, p_2, \ldots$ is the sequence of primes written in their natural order.

† For a description of torsion-free abelian groups in terms of matrices see [b25].

If g is an element of an abelian group G, the *height vector* of g is $\mathbf{h}(g) = (h_1, h_2, \ldots)$ where h_i is the p_i-height of g in G. Each h_i is therefore ∞ or a nonnegative integer. Any vector $\mathbf{h}$ with components of this sort will be called a height without reference to a particular abelian group.

The set of all heights may be partially ordered by defining $\mathbf{h} \leq \mathbf{h}'$ to mean that $h_i \leq h_i'$ for all i: here the symbol ∞ is subject to the usual rules. Thus $\mathbf{0} = (0, 0, \ldots)$ is the unique minimum height and $\boldsymbol{\infty} = (\infty, \infty, \ldots)$ the unique maximum height.

If g is a group element with p-height h, then pg has p-height $h + 1$. Thus if the p-height of an element g of G is increased for finitely many primes p, the resulting height will be that of a multiple of g. This might suggest that such heights be regarded as equivalent.

Accordingly two heights $\mathbf{h}$ and $\mathbf{h}'$ will be called *equivalent* if $h_i = h_i'$ for almost all i and $h_i = h_i'$ whenever h_i or h_i' is infinite. One readily verifies that this is an equivalence relation on the set of heights. The equivalence classes are termed *types*. The *type of a group element* g is defined to be the type of its height vector: this will be denoted by

$$\mathbf{t}(g).$$

The set of all types can also be partially ordered: we define $\mathbf{t} \leq \mathbf{t}'$ to mean that $\mathbf{h} \leq \mathbf{h}'$ where $\mathbf{h}$ and $\mathbf{h}'$ are some heights belonging to the types $\mathbf{t}$ and $\mathbf{t}'$ respectively. It is easy to check the axioms for a partial order. Clearly there is a unique minimum and a unique maximum type.

Torsion-Free Groups of Rank 1

Let us see how the concept of type may be applied to torsion-free groups of rank 1: note that such groups are essentially subgroups of $\mathbb{Q}$.

Suppose that G is a torsion-free abelian group of rank ≤ 1 and let g_1, g_2 be two nonzero elements of G. Then $\langle g_1 \rangle \cap \langle g_2 \rangle \neq 0$ since $\{g_1, g_2\}$ must be dependent. Thus $0 \neq m_1 g_1 = m_2 g_2$ for certain integers m_i. It follows from the definition that $\mathbf{h}(g_1)$ and $\mathbf{h}(g_2)$ are equivalent and hence that $\mathbf{t}(g_1) = \mathbf{t}(g_2)$. Thus all nonzero elements of G have the same type, which is referred to as the *type of* G, in symbols $\mathbf{t}(G)$.

4.4.1 (Baer). *Two torsion-free abelian groups of* rank ≤ 1 *are isomorphic if and only if they have the same type. Moreover every type is the type of some torsion-free abelian group of* rank 0 *or* 1.

Proof. Suppose that G and H are two torsion-free abelian groups of rank 1 with the same type. Let $0 \neq a \in G$ and $0 \neq b \in H$: then $\mathbf{h}(a) = (k_1, k_2, \ldots)$ and $\mathbf{h}(b) = (l_1, l_2, \ldots)$ belong to the same type. The height vectors differ in only finitely many components, say at $n_1, n_2, \ldots, n_s$. Let us write $k(i) = k_{n_i}$ and $l(i) = l_{n_i}$; then $k(i)$ and $l(i)$ are unequal integers and we can write

$a = p_{n_1}^{k(1)} \cdots p_{n_s}^{k(s)} a'$ and $b = p_{n_1}^{l(1)} \cdots p_{n_s}^{l(s)} b'$ for some a' in G and b' in H. Now $\mathbf{h}(a') = \mathbf{h}(b')$; consequently the equation $mx = na'$ has a solution for x in G if and only if $my = nb'$ has a solution for y in H. Moreover these equations have a unique solution for given m and n if they have any solution. The assignment $x \mapsto y$ is a bijection from G to H since every element of G or H is realized as a solution of some such equation. This bijection is easily seen to be a homomorphism, so $G \simeq H$.

Finally let $\mathbf{t}$ be any type and let $\mathbf{h} = (h_1, h_2, \ldots)$ be any height in $\mathbf{t}$. Define G to be the subgroup of $\mathbb{Q}$ generated by the rational numbers $1/p_i^j$, $i = 1, 2, \ldots$, $j = 0, 1, \ldots, h_i$. Clearly 1 has height $\mathbf{h}$ in G, so $\mathbf{t}(G) = \mathbf{t}(1) = \mathbf{t}$ and our theorem is proven. □

For example $\mathbb{Z}$ has the type of $(0, 0, \ldots)$ and $\mathbb{Q}$ has the type of $(\infty, \infty, \ldots)$. The group of all *dyadic* rationals $m2^n$, $(m, n \in \mathbb{Z})$, has the type of $(\infty, 0, 0, \ldots)$. It is clear that the set of isomorphism classes of torsion-free abelian groups of rank 1 has the cardinality $2^{\aleph_0}$.

Indecomposable Torsion-Free Abelian Groups

Whereas an indecomposable abelian torsion group is either cyclic or quasicyclic (4.3.12), it is a measure of the difficulty of the theory of torsion-free abelian groups that indecomposable groups can have rank greater than 1. In fact such examples are relatively common.

4.4.2. *There exist indecomposable torsion-free abelian groups of rank* 2 *which have exactly two automorphisms.*

Proof. Let V be a rational vector space of dimension 2 and let $\{u, v\}$ be a basis for V. Choose three distinct primes p, q, r and define G to be the subgroup of V generated by all elements of the form

$$p^m u, \qquad q^m v, \qquad r^m(u + v),$$

where m assumes all integral values. Certainly G is a torsion-free abelian group of rank 2.

Our first object is to show that the only elements with infinite p-height in G are rational multiples of u. To this end suppose that

$$g = ip^l u + jq^m v + kr^n(u + v)$$

has infinite p-height: here i, j, k, l, m, n are integers. For any positive integer t there is a $\bar{g}$ in G such that $g = p^t \bar{g}$; write $\bar{g}$ in the form

$$\bar{i}p^{\bar{l}}u + \bar{j}q^{\bar{m}}v + \bar{k}r^{\bar{n}}(u + v).$$

Since u and v are independent, the coefficients of v in g and $p^t\bar{g}$ are equal; thus $jq^m + kr^n = p^t(\bar{j}q^{\bar{m}} + \bar{k}r^{\bar{n}})$. Hence the rational number $(jq^m + kr^n)p^{-t}$

involves no positive power of p in its denominator, no matter how large t is. This can only mean that $jq^m + kr^n = 0$, so that $g = (ip^l + kr^n)u$ as claimed. In a similar way one proves that elements of infinite q- or r-height are rational multiples of v or $u + v$ respectively.

The information just obtained can be used to identify the automorphisms of G. If $\alpha \in \text{Aut } G$, then u and $u\alpha$ have the same p-height; therefore $u\alpha = du$ where d is rational. For similar reasons $v\alpha = ev$ and $(u + v)\alpha = f(u + v)$ with e and f rational. But $(u + v)\alpha = u\alpha + v\alpha$, so $d = e = f$ and hence $x\alpha = dx$ for all x in G. Since du and dv have to belong to G, inspection of the generators of G reveals that d is an integer. Also α^{-1} exists, so $d = \pm 1$. The mapping $x \mapsto -x$ *is* an automorphism α of G; therefore Aut G has order 2, being generated by this α.

Finally, suppose $G = H \oplus K$ where $H \neq 0$ and $K \neq 0$. The assignments $h \mapsto -h$, $k \mapsto k$, $(h \in H, k \in K)$, determine a nontrivial automorphism of G that does not equal α. By this contradiction G is indecomposable. □

It should be apparent to the reader that by increasing the number of primes in the preceding example indecomposable torsion-free abelian groups of all countable ranks may be constructed.

Pontryagin's Criterion for Freeness

In certain contexts the following criterion is useful.

4.4.3 (Pontryagin). *Let G be a countable torsion-free abelian group. Then G is free abelian if and only if every subgroup with finite rank is free abelian.*

Proof. Necessity of the condition follows from 4.2.3. Assume that G is not free abelian but that every subgroup of finite rank is. Let $\{g_1, g_2, \ldots\}$ be a countable set of generators of G and define G_1 to consist of all x in G such that $mx \in \langle g_1 \rangle$ for some $m > 0$. Clearly G_1 has rank 1, so it is infinite cyclic by hypothesis. Now G/G_1 is torsion-free and countable. Moreover its subgroups of finite rank are free abelian: for if H/G_1 is such a subgroup, H has finite rank and is therefore free abelian and finitely generated; thus H/G_1 is free abelian, being finitely generated and torsion-free. Consequently, G/G_1 inherits the hypothesis on G.

In the same way define G_2/G_1 to consist of all $x + G_1$ such that $m(x + G_1) \in \langle g_2 + G_1 \rangle$ for some positive m. Then G_2/G_1 is infinite cyclic and G/G_2 inherits the hypothesis on G. Continuing in this manner we construct a countable ascending chain of subgroups $G_1 < G_2 < \cdots$ with union G such that G_{i+1}/G_i is infinite cyclic. Now write $G_{i+1} = G_i \oplus \langle x_{i+1} \rangle$. Then it is evident that $x_1, x_2, \ldots$ generate G and that these elements form an independent set. Hence G is a free abelian group on $\{x_1, x_2, \ldots\}$. □

Thus if a countable torsion-free abelian group is not free abelian, the trouble must already occur in a subgroup of finite rank. The same cannot be said of uncountable groups, as we shall soon see.

Cartesian Sums of Infinite Cyclic Groups

Cartesian sums of torsion-free abelian groups of rank 1 form an interesting class of groups sometimes called *vector groups*. For simplicity we shall discuss only cartesian sums of infinite cyclic groups. Such groups are not free abelian but they come rather close to having this property.

4.4.4 (Specker). *Let G be a cartesian sum of infinitely many infinite cyclic groups. Then G is not expressible as a direct sum of indecomposable groups. In particular G is not free abelian.*

Proof. Let $G = \mathrm{Cr}_{\lambda \in \Lambda} X_\lambda$ where X_λ is infinite cyclic and Λ is infinite. Suppose that $G = \mathrm{Dr}_{i \in I} G_i$ where G_i is indecomposable and nontrivial. If K_λ denotes the kernel of the natural projection $G \to X_\lambda$, then $\bigcap_\lambda K_\lambda = 0$ and G/K_λ is infinite cyclic. Hence $G_i \not\leq K_\lambda$ for some λ and $G_i/(G_i \cap K_\lambda)$ is infinite cyclic, whence $G_i \cap K_\lambda$ is a direct summand of the indecomposable group G_i. Thus $G_i \cap K_\lambda = 0$ and G_i is infinite cyclic. Consequently G is free abelian: we must show this to be impossible. By 4.2.3 subgroups of G are also free abelian, so we can replace Λ by a countably infinite subset. Henceforth assume that Λ is countable, equal to $\{1, 2, \dots\}$ say: note that G is uncountable while $D = \mathrm{Dr}_{i=1,2,\dots} X_i$ is countable.

Let H be the subgroup consisting of all h in G such that for each positive integer i almost all the components of h are divisible by 2^i. If $h \in H$, then we can find an element d of D such that $h - d \in 2H$. Hence $H \leq D + 2H$ and $|H : 2H| \leq |D|$, which is countable. Since H is free abelian, it is countable. But this is incorrect since H has an uncountable subgroup, namely $\mathrm{Cr}_{i=1,2,\dots} 2^i X_i$. □

We show next that the group G has the remarkable property that each of its countable subgroups is free abelian. This will be an easy consequence of the following result.

4.4.5 (Specker). *Let G be a cartesian sum of infinite cyclic groups. Then every finite subset of G is contained in a finitely generated direct summand of G whose direct complement is also a cartesian sum of infinite cyclic groups.*

Proof. Let $G = \mathrm{Cr}_{\lambda \in \Lambda} X_\lambda$ where $X_\lambda = \mathbb{Z}$, and let $\{g^{(1)}, \dots, g^{(n)}\}$ be a finite subset of G. The theorem will be proved by induction on n. Consider first the case $n = 1$ and let $g^{(1)} \neq 0$. Define k to be the smallest absolute value of a non-zero component of $g^{(1)}$. If $k = 1$, then $g_\lambda^{(1)} = \pm 1$ for some λ: in this

case if K_λ is the kernel of the projection $G \to G_\lambda$, then plainly $G = \langle g^{(1)} \rangle \oplus K_\lambda$; of course $K_\lambda \simeq \mathrm{Cr}_{\mu \neq \lambda} X_\mu$. Now let $k > 1$.

Write $g_\lambda^{(1)}$ in the form $kq_\lambda + r_\lambda$ where q_λ, r_λ are integers and $0 \leq r_\lambda < k$, and define elements x, y of G by the rules $x_\lambda = q_\lambda$ and $y_\lambda = r_\lambda$. Thus $g^{(1)} = kx + y$. Now $g_{\lambda_0}^{(1)} = \pm k$ for some λ_0 in Λ; then $q_{\lambda_0} = \pm 1$ and $r_{\lambda_0} = 0$, so that $|x_{\lambda_0}| = 1$. The argument of the first paragraph shows that $G = \langle x \rangle \oplus K_{\lambda_0}$. Now $y \in K_{\lambda_0}$ because $r_{\lambda_0} = 0$, and clearly the smallest $|y_\lambda|$ is less than k. Hence induction on k gives $K_{\lambda_0} = L \oplus M$ where L is finitely generated and contains y and M is a cartesian sum of infinite cyclic groups. Thus $g^{(1)} = kx + y \in \langle x \rangle \oplus L$ and $G = \langle x \rangle \oplus L \oplus M$.

Now let $n > 1$ and assume that $g^{(1)}, \ldots, g^{(n-1)}$ are contained in a finitely generated subgroup G_1 and that $G = G_1 \oplus G_2$ where G_2 is a cartesian sum of infinite cyclic groups. Write $g^{(n)} = x + y$ with $x \in G_1$ and $y \in G_2$. Then y belongs to a finitely generated subgroup G_3 such that $G_2 = G_3 \oplus G_4$ and G_4 is a cartesian sum of infinite cyclic groups. Finally $G = G_1 \oplus G_3 \oplus G_4$ and all the $g^{(i)}$ belong to $G_1 \oplus G_3$. □

4.4.6 (Specker). *If G is a cartesian sum of infinite cyclic groups, every countable subgroup of G is free abelian.*

Proof. Let H be a countable subgroup which is not free. By 4.4.3 there exists a subgroup K of H with finite rank which is not free. Let S be a maximal independent subset of K. Then S is finite and thus lies in a finitely generated direct summand D of G, by 4.4.5. If $k \in K$, then $mk \in \langle S \rangle \leq D$ for some $m > 0$. But G/D is torsion-free, so $k \in D$ and $K \leq D$. Now D is free abelian, being finitely generated (4.2.10), so K is free abelian, a contradiction. □

Taking 4.4.4 and 4.4.6 together we see that Pontryagin's criterion is not valid for uncountable groups.

Exercises 4.4

*1. (a) If G and H are torsion-free abelian groups of rank 1, show that G is isomorphic with a subgroup of H if and only if $\mathbf{t}(G) \leq \mathbf{t}(H)$.
   (b) Prove that if G is isomorphic with a subgroup of H and H is isomorphic with a subgroup of G, then $G \simeq H$ (where G and H are as in (a)).

2. Show that the conclusion of Exercise 4.4.1 (b) is not valid for torsion-free abelian groups of rank 2. [*Hint*: let A and B be the additive groups of all $m3^n$ and $m5^n$, $(m, n \in \mathbb{Z})$, respectively. Consider $G = A \oplus B$ and $H = \langle a + b, 2G \rangle$ where $a \in A \backslash 2A$ and $b \in B \backslash 2B$.]

3. If G is a torsion-free abelian group of rank 1, describe Aut G and End G in terms of the type of G. When is Aut G finite?

4. Show that there exist $2^{\aleph_0}$ torsion-free abelian groups of rank 1, say $\{G_\lambda | \lambda \in \Lambda\}$, such that $\mathrm{Hom}(G_\lambda, G_\mu) = 0$ if $\lambda \neq \mu$.

5. Find torsion-free abelian groups whose automorphism groups are elementary abelian 2-groups of cardinality $2^{\aleph_0}$ and $2^{2^{\aleph_0}}$ respectively.

6. Construct an indecomposable torsion-free abelian group of rank r for each countable r.

*7. A group is called a *minimax group* if it has a series of finite length whose factors satisfy max *or* min.
   (a) Prove that an abelian group G is a minimax group if and only if it has a finitely generated subgroup H such that G/H has min.
   (b) Show that the torsion-subgroup of an abelian minimax group has min and is a direct summand.
   (c) Let G be a torsion-free abelian minimax group. Prove that G has a finitely generated free abelian subgroup H such that G/H is a divisible group with min. If K is another such subgroup, prove that $H \simeq K$ and $G/H \simeq G/K$.
   (d) Characterize subgroups of $\mathbb{Q}$ that are minimax groups: hence characterize torsion-free abelian minimax groups.

8. (Sasiada). Let G be a countable reduced torsion-free abelian group and let C be a cartesian sum of countably many infinite cyclic groups. If $\alpha: C \to G$ is a homomorphism, prove that $a_i\alpha = 0$ for almost all i where a_i is the element of C whose ith component is 1 and other components are 0. [*Hint*: Assume that $a_i\alpha \neq 0$ for all i. Find a sequence of integers $1 = n_1 < n_2 < \cdots$ such that $(n_i!)a_i\alpha \notin n_{i+1}G$. Now argue that there is an $h = (h_1, h_2, \ldots) \neq 0$ in C such that $h\alpha = 0$ and $h_i = 0$ or $\pm n_i!$. Let m be the smallest integer such that $h_m \neq 0$ and write $h_m a_m = h - (0, 0, \ldots, 0, h_{m+1}, \ldots)$.] *Remark*: Groups with the property just established for G are called *slender groups*.

9. (Łoś). Let C and G be as in Exercise 4.4.8. Let D be the direct sum of the infinite cyclic groups.
   (a) If $\alpha: C \to G$ is a homomorphism that vanishes on D, prove that $\alpha = 0$.
   (b) Prove that C/D does not have G as a homomorphic image if $G \neq 1$.
   [*Hint*: To prove (a) suppose that $x\alpha \neq 0$ where $x = (m_1, m_2, \ldots)$. Define a homomorphism $\beta: D \to C$ by the rule $a_i\beta = (0, 0, \ldots, 0, m_i, m_{i+1}, \ldots)$. Prove that $a_i\beta\alpha \neq 0$.]

CHAPTER 5

Soluble and Nilpotent Groups

In this chapter we shall study classes of groups which can be constructed from abelian groups by repeatedly forming extensions, the process by which finite groups are built up from simple groups.

5.1. Abelian and Central Series

Definition. A group G is said to be *soluble* (or *solvable*) if it has an *abelian series*, by which we mean a series $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ in which each factor G_{i+1}/G_i is abelian.

Naturally every abelian group is soluble. The first example of a non-abelian soluble group is the symmetric group S_3.

Definitions. If G is a soluble group, the length of a shortest abelian series in G is called the *derived length* of G. Thus G has derived length 0 if and only if it has order 1. Also the groups with derived length at most 1 are just the abelian groups. A soluble group with derived length at most 2 is said to be *metabelian.*

We record next some of the most elementary properties of soluble groups.

5.1.1. *The class of soluble groups is closed with respect to the formation of subgroups, images, and extensions of its members.*

Proof. Let G be a soluble group with an abelian series $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$. If H is a subgroup of G, then by the Second Isomorphism

Theorem $H \cap G_{i+1}/H \cap G_i \simeq (H \cap G_{i+1})G_i/G_i \leq G_{i+1}/G_i$, which shows that $\{H \cap G_i | i = 0, 1, \ldots, n\}$ is an abelian series of H and H is soluble. If $N \lhd G$, then $G_{i+1}N/G_iN \simeq G_{i+1}/G_{i+1} \cap (G_iN)$, which is an image of G_{i+1}/G_i. By the Third Isomorphism Theorem $\{G_iN/N | i = 0, 1, \ldots, n\}$ is an abelian series of G/N, so this is a soluble group. The third statement is obvious. □

5.1.2. *The product of two normal soluble subgroups of a group is soluble.*

Proof. Let $M \lhd G$ and $N \lhd G$ where M and N are soluble. Then 5.1.1 shows that $MN/N \simeq M/M \cap N$ is soluble. Hence MN is soluble. □

It follows that every finite group G has a unique maximal normal soluble subgroup, namely the product S of all normal soluble subgroups, the *soluble radical* of G. Since G/S is clearly semisimple, *every finite group is an extension of a soluble group by a semisimple group.*

An abelian series of a finite group can be refined to a composition series whose factors are abelian simple groups, and hence are of prime order. Thus *a finite group is soluble if and only if it has a series whose factors are cyclic groups with prime orders.* However, despite the fact that finite soluble groups can be constructed from such elementary groups, their structure is by no means obvious.

Definitions. A group G is called *nilpotent* if it has a *central series*, that is, a normal series $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ such that G_{i+1}/G_i is contained in the center of G/G_i for all i. The length of a shortest central series of G is the *nilpotent class* of G.

A nilpotent group of class 0 has order 1 of course, while nilpotent groups of class at most 1 are abelian. Whereas nilpotent groups are obviously soluble, an example of a nonnilpotent soluble group is S_3 (its centre is trivial). The great source of finite nilpotent groups is the class of groups whose orders are prime powers.

5.1.3. *A finite p-group is nilpotent.*

Proof. Let G be a finite p-group of order >1. Then 1.6.14 shows that $\zeta G \neq 1$. Hence $G/\zeta G$ is nilpotent by induction on $|G|$. By forming the preimages of the terms of a central series of $G/\zeta G$ under the natural homomorphism $G \to G/\zeta G$ and adjoining 1, we arrive at a central series of G. □

5.1.4. *The class of nilpotent groups is closed under the formation of subgroups, images, and finite direct products.*

The proof is left to the reader as an exercise.

Commutators

To make progress in the subject it is necessary to develop a systematic calculus of commutators.

Let G be a group and let $x_1, x_2, \ldots$ be elements of G. Recall that the *commutator* of x_1 and x_2 is

$$[x_1, x_2] = x_1^{-1}x_2^{-1}x_1x_2 = x_1^{-1}x_1^{x_2}.$$

More generally, *a simple commutator of weight* $n \geq 2$ is defined recursively by the rule

$$[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n],$$

where by convention $[x_1] = x_1$. A useful shorthand notation is

$$[x, {}_n y] = [x, \underbrace{y, \ldots, y}_{n}].$$

We list now the basic properties of commutators.

5.1.5. *Let x, y, z be elements of a group. Then*:

(i) $[x, y] = [y, x]^{-1}$;
(ii) $[xy, z] = [x, z]^y[y, z]$ *and* $[x, yz] = [x, z][x, y]^z$;
(iii) $[x, y^{-1}] = ([x, y]^{y^{-1}})^{-1}$ *and* $[x^{-1}, y] = ([x, y]^{x^{-1}})^{-1}$;
(iv) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$ (*the Hall–Witt identity*).

Proof. The first three parts are easily checked. (iv) is most conveniently proved by setting $u = xzx^{-1}yx$, $v = yxy^{-1}zy$, and $w = zyz^{-1}xz$, and observing that $[x, y^{-1}, z]^y = u^{-1}v$, $[y, z^{-1}, x]^z = v^{-1}w$ and $[z, x^{-1}, y]^x = w^{-1}u$; the identity is then obvious. □

Commutator Subgroups

It is useful to be able to form commutators of subsets as well as elements. Let $X_1, X_2, \ldots$ be nonempty subsets of a group G. Define the *commutator subgroup* of X_1 and X_2 to be

$$[X_1, X_2] = \langle [x_1, x_2] | x_1 \in X_1, x_2 \in X_2 \rangle.$$

More generally, let

$$[X_1, \ldots, X_n] = [[X_1, \ldots, X_{n-1}], X_n]$$

where $n \geq 2$. Observe that $[X_1, X_2] = [X_2, X_1]$ by 5.1.5(i). It is sometimes convenient to write $[X, {}_n Y]$ for $[X, \underbrace{Y, \ldots, Y}_{n}]$.

It is natural to introduce an analogue of the conjugate of an element. Accordingly we define

$$X_1^{X_2} = \langle x_1^{x_2} = x_2^{-1}x_1x_2 \mid x_1 \in X_1, x_2 \in X_2 \rangle.$$

If X is a subset and H is a subgroup of a group, then $X \subseteq X^H \lhd \langle X, H\rangle$. Thus $X^H = X^{\langle X, H\rangle}$ is precisely the normal closure of X in $\langle X, H\rangle$ and the notation is consistent with that used previously for normal closures.

5.1.6. *Let X be a subset and K a subgroup of a group.*

(i) $X^K = \langle X, [X, K]\rangle$.
(ii) $[X, K]^K = [X, K]$.
(iii) *If* $K = \langle Y\rangle$, *then* $[X, K] = [X, Y]^K$.

Proof. (i) This follows from the identity $x^k = x[x, k]$.

(ii) The subgroup $[X, K]^K$ is generated by all $[x, k_1]^{k_2}$, where $x \in X$ and $k_i \in K$. Now 5.1.5 shows that $[x, k_1]^{k_2} = [x, k_2]^{-1}[x, k_1k_2]$, so $[x, k_1]^{k_2} \in [X, K]$ and $[X, K]^K = [X, K]$.

(iii) By (ii) it is enough to show that $[x, k] \in [X, Y]^K$ for all x in X and k in K. Now we may write $k = y_1^{\varepsilon_1}y_2^{\varepsilon_2}\cdots y_r^{\varepsilon_r}$ where $y_i \in Y$ and $\varepsilon_i = \pm 1$. Firstly $[x, y_1^{-1}] = ([x, y_1]^{y_1^{-1}})^{-1} \in [X, Y]^K$, so $[x, k] \in [X, Y]^K$ if $r = 1$. Let $r > 1$ and put $k' = y_1^{\varepsilon_1}\cdots y_{r-1}^{\varepsilon_{r-1}}$. Then $[x, k] = [x, k'y_r^{\varepsilon_r}] = [x, y_r^{\varepsilon_r}][x, k']^{y_r^{\varepsilon_r}}$, a product which belongs to $[X, Y]^K$ by induction on r. □

5.1.7. *Let H and K be subgroups of a group. If $H = \langle X\rangle$ and $K = \langle Y\rangle$, then $[H, K] = [X, Y]^{HK}$.*

This follows from 5.1.6 (iii).

The Derived Series

Recall that G' is the derived subgroup of the group G, being generated by all commutators in G: thus $G' = [G, G]$. By repeatedly forming derived subgroups a descending sequence of fully-invariant subgroups is generated:

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots$$

where $G^{(n+1)} = (G^{(n)})'$. This is called the *derived series* of G, although it need not reach 1 or even terminate. Of course all the factors $G^{(n)}/G^{(n+1)}$ are abelian groups: the first of these, G/G', is of particular importance and is often written G_{ab} since it is the largest abelian quotient group of G.

5.1.8. *If $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ is an abelian series of a soluble group G, then $G^{(i)} \leq G_{n-i}$. In particular $G^{(n)} = 1$. The derived length of G is equal to the length of the derived series of G.*

Proof. The inclusion is certainly true if $i = 0$; assume that it is valid for i. Then $G^{(i+1)} = (G^{(i)})' \leq (G_{n-i})' \leq G_{n-(i+1)}$ since $G_{n-i}/G_{n-(i+1)}$ is abelian. It follows that no abelian series can be shorter than the derived series. □

According to 5.1.8 a group is soluble if and only if its derived series reaches the identity subgroup after a finite number of steps. By the same result every soluble group has a *normal abelian series*, that is to say, an abelian series all of whose terms are normal subgroups, the derived series being an example.

The Lower and Upper Central Series

There is another natural way of generating a descending sequence of commutator subgroups of a group, by repeatedly commuting with G. There results a series

$$G = \gamma_1 G \geq \gamma_2 G \geq \cdots$$

in which $\gamma_{n+1} G = [\gamma_n G, G]$. This is called the *lower central series* of G: notice that $\gamma_n G/\gamma_{n+1} G$ lies in the center of $G/\gamma_{n+1} G$ and that each $\gamma_n G$ is fully-invariant in G. Like the derived series the lower central series does not in general reach 1. The reader should keep in mind that $\gamma_1 G$ is the first term of the lower central series whereas $G^{(0)}$ is the first term of the derived series.

There is an ascending sequence of subgroups that is dual to the lower central series in the same sense that the center is dual to the commutator subgroup. This is the *upper central series*

$$1 = \zeta_0 G \leq \zeta_1 G \leq \zeta_2 G \leq \cdots,$$

defined by $\zeta_{n+1} G/\zeta_n G =$ the center of $G/\zeta_n G$. Each $\zeta_n G$ is characteristic but not necessarily fully-invariant in G. Of course $\zeta_1 G = \zeta G$. This series need not reach G, but if G is finite, the series terminates at a subgroup called the *hypercenter*.

The crucial properties of these central series are displayed in the next result.

5.1.9. *Let $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ be a central series in a nilpotent group G. Then*:

(i) $\gamma_i G \leq G_{n-i+1}$, *so that* $\gamma_{n+1} G = 1$;
(ii) $G_i \leq \zeta_i G$, *so that* $\zeta_n G = G$;
(iii) *the nilpotent class of G = the length of the upper central series = the length of the lower central series.*

Proof. (i) This is clear if $i = 1$. Since G_{n-i+1}/G_{n-i} lies in the center of G/G_{n-i}, we have $[G_{n-i+1}, G] \leq G_{n-i}$. By induction $\gamma_{i+1} G = [\gamma_i G, G] \leq [G_{n-i+1}, G] \leq G_{n-i}$ as required.

(ii) The proof is another easy induction.

(iii) By (i) and (ii) the upper and lower central series are shortest central series of G. □

In particular, a group is nilpotent if and only if the lower central series reaches the identity subgroup after a finite number of steps or, equivalently, the upper central series reaches the group itself after a finite number of steps.

5.1.10 (The Three Subgroup Lemma: Kalužnin, P. Hall). *Let H, K, L, be subgroups of a group G. If two of the commutator subgroups $[H, K, L]$, $[K, L, H]$, $[L, H, K]$ are contained in a normal subgroup of G, then so is the third.*

Proof. By 5.1.7 the group $[H, K, L]$ is generated by conjugates of commutators of the form $[h, k^{-1}, l]$, $h \in H$, $k \in K$, $l \in L$, with similar statements for $[K, L, H]$ and $[L, H, K]$. The Hall–Witt identity (5.1.5) shows that if two of $[h, k^{-1}, l]$, $[k, l^{-1}, h]$, $[l, h^{-1}, k]$ belong to a normal subgroup of G, so does the third. This implies the result. □

The Three Subgroup Lemma enables us to establish several useful commutator properties of the upper and lower central series.

5.1.11. *Let G be any group and let i and j be positive integers.*

(i) $[\gamma_i G, \gamma_j G] \leq \gamma_{i+j} G$.
(ii) $\gamma_i(\gamma_j G) \leq \gamma_{ij} G$.
(iii) $[\gamma_i G, \zeta_j G] \leq \zeta_{j-i} G$ *if* $j \geq i$.
(iv) $\zeta_i(G/\zeta_j G) = \zeta_{i+j} G/\zeta_j G$.

Proof. (i) Use induction on j, the case $j = 1$ being clear. Lemma 5.1.10 shows that $[\gamma_i G, \gamma_{j+1} G] = [\gamma_j G, G, \gamma_i G]$ is contained in the product

$$[G, \gamma_i G, \gamma_j G][\gamma_i G, \gamma_j G, G]:$$

by induction the latter is contained in $\gamma_{i+j+1} G$.

(ii) Use induction on i, the case $i = 1$ being obvious. Then $\gamma_{i+1}(\gamma_j G) = [\gamma_i(\gamma_j G), \gamma_j G] \leq [\gamma_{ij} G, \gamma_j G] \leq \gamma_{(i+1)j}$ by (i).

(iii) This is clear if $i = 1$. Now by 5.1.10 we have

$$[\gamma_{i+1} G, \zeta_j G] = [\gamma_i G, G, \zeta_j G] \leq [G, \zeta_j G, \gamma_i G][\zeta_j G, \gamma_i G, G],$$

a product which is contained in $\zeta_{j-(i+1)} G$ by induction on i.

(iv) Use induction on i. □

5.1.12. *If G is any group, then $G^{(i)} \leq \gamma_{2^i} G$. If G is nilpotent with positive class c, its derived length is at most $[\log_2 c] + 1$.*

Proof. The first part follows on applying 5.1.11(ii) to $G^{(i)} = \gamma_2(\cdots(\gamma_2 G)\cdots)$ where γ_2 is taken i times. Now let G be nilpotent with class $c > 0$ and let d be the derived length; then $G^{(i)} \leq \gamma_{2^i} G \leq \gamma_{c+1} G = 1$ provided $2^i \geq c + 1$. The smallest such i is $[\log_2 c] + 1$, whence $d \leq [\log_2 c] + 1$. □

Triangular and Unitriangular Groups

We conclude this section with a well-known ring-theoretic source of examples of nilpotent groups. Let S be a ring with identity and let N be a subring of S. Write $N^{(i)}$ for the set of all *sums of products of i elements of N* where $i > 0$; clearly $N^{(i)}$ is a subring. Also $N^{(i)} = 0$ if and only if all products of i elements of N vanish. If some $N^{(i)}$ equals 0, then N is said to be *nilpotent*.

Assume that $N^{(n)} = 0$ and let U be the set of all elements of the form $1 + x$ where $x \in N$. Then U is a group with respect to the ring multiplication; for

$$(1 + x)(1 + y) = 1 + (x + y + xy) \in U$$

and

$$(1 + x)^{-1} = 1 + (-x + x^2 - \cdots + (-1)^{n-1}x^{n-1}) \in U:$$

here it is relevant that $x^n = 0$. Put $U_i = \{1 + x | x \in N^{(i)}\}$. We shall prove that $1 = U_n \leq U_{n-1} \leq \cdots \leq U_1 = U$ is a central series of U. In the first place U_i is a subgroup because $N^{(i)}$ is a subring. Let $x \in N^{(r)}$ and $y \in N^{(s)}$; then

$$\begin{aligned}[1 + x, 1 + y] &= ((1 + y)(1 + x))^{-1}(1 + x)(1 + y)\\ &= (1 + y + x + yx)^{-1}(1 + x + y + xy).\end{aligned}$$

Setting $u = x + y + xy$ and $v = y + x + yx$, we have

$$\begin{aligned}[1 + x, 1 + y] &= (1 - v + v^2 - \cdots + (-1)^{n-1}v^{n-1})(1 + u)\\ &= 1 + (1 - v + v^2 - \cdots + (-1)^{n-2}v^{n-2})(u - v) + (-1)v^{n-1}u.\end{aligned}$$

This is in U_{r+s} since $v^{n-1}u \in N^{(n)} = 0$ and $u - v = xy - yx \in N^{(r+s)}$. Therefore $[U_r, U_s] \leq U_{r+s}$ and in particular $[U_r, U] \leq U_{r+1}$, which shows that the U_r's form a central series and U is nilpotent of class $\leq n - 1$.

For example, let us take S to be the ring of all $n \times n$ matrices over R (a commutative ring with identity) and let N be the subring of *upper zero triangular matrices*: these are matrices with 0 on and below the diagonal. By matrix multiplication we see that $N^{(2)}$ consists of all elements of N whose first superdiagonal is zero, $N^{(3)}$ of all elements whose first two superdiagonals are zero and so on: hence $N^{(n)} = 0$. Here the group U is just $U(n, R)$, *the group of all* $n \times n$ (upper) *unitriangular matrices* over R, that is matrices with 1 on the diagonal and 0 below it. In fact U has nilpotent class exactly $n - 1$ since $[1 + E_{12}, 1 + E_{23}, \ldots, 1 + E_{n-1n}] = 1 + E_{1n} \neq 1$. It follows that there exist nilpotent groups of arbitrary class.

Observe that U_i consists of all unitriangular matrices whose first $i - 1$ superdiagonals are 0; from this it is easy to see that

$$U_i/U_{i+1} \simeq \underbrace{R \oplus \cdots \oplus R}_{n-i}.$$

Taking $R = \mathrm{GF}(p)$, we find that $U = U(n, p)$ is a finite p-group of order $p^{n(n-1)/2}$. On the other hand, if $R = \mathbb{Z}$, then U is a torsion-free nilpotent group: in fact U is also finitely generated, by the $1 + E_{ii+1}$, $i = 1, 2, \ldots, n - 1$, for example (Exercise 5.1.14).

Finally let $T = T(n, R)$ denote the set of all *upper triangular matrices* over R; these are matrices with 0 below the diagonal and units of R on the diagonal. Such a matrix is invertible since its determinant is a unit of R: clearly T is a subgroup of $GL(n, R)$. We can define a function

$$\theta: T \to \underbrace{R^* \times \cdots \times R^*}_{n}$$

by mapping a matrix onto its principal diagonal. Matrix multiplication shows that θ is an epimorphism whose kernel is precisely $U = U(n, R)$. Since $U \lhd T$ and T/U is abelian, T is a soluble group. Using 5.1.12 one sees that the derived length of T is at most $[\log_2(n - 1)] + 2$ if $n > 1$.

Exercises 5.1

1. Prove that S_n is soluble if and only if $n < 5$.
2. Prove 5.1.4.
3. Verify the commutator identities (i)–(iii) in 5.1.5.

*4. Show that the identity $[u^m, v] = [u, v]^{u^{m-1}+u^{m-2}+\cdots+u+1}$ holds in any group (here $x^{y+z} = x^y x^z$). Deduce that if $[u, v]$ belongs to the center of $\langle u, v\rangle$, then $[u^m, v] = [u, v]^m = [u, v^m]$.

5. If H, K, L are normal subgroups of a group, then $[HK, L] = [H, L][K, L]$.
6. Suppose that G is a nilpotent group which is not abelian and let $g \in G$. Show that the nilpotent class of $\langle g, G'\rangle$ is smaller than that of G. Deduce that G can be expressed as a product of normal subgroups of smaller class.

*7. If $G = HN'$ where $H \leq G$ and $N \lhd G$, then $G = H(\gamma_i N)$ for all i. [*Hint*: Use $N = (H \cap N)N'$.]

8. A finite nilpotent group has a central series with factors of prime order.
9. Show that the class of a nilpotent group cannot be bounded by a function of the derived length.
10. Show that $T(2, \mathbb{Z}) \simeq D_\infty \times \mathbb{Z}_2$ where D_∞ is the infinite dihedral group.

*11. Prove that $U(n, p) \equiv U(n, \mathrm{GF}(p))$ is a Sylow p-subgroup of $\mathrm{GL}(n, p)$. Deduce that every finite p-group is isomorphic with a subgroup of some $U(n, p)$.

12. If $n > 1$ and F is any field, the derived length of $T(n, F)$ equals $[\log_2(n-1)] + 2$.

*13. Let R be a commutative ring with identity and put $U = U(n, R)$. Define U_i to be the set of elements of U having (at least) $i - 1$ zero superdiagonals. Prove that $1 = U_n < U_{n-1} < \cdots < U_1 = U$ is both the upper and the lower central series of U.

*14. Prove that $U(n, \mathbb{Z}) = \langle 1 + E_{12}, \ldots, 1 + E_{n-1n} \rangle$ where $n > 1$.

15. (Sherman). Let G be a nontrivial finite nilpotent group. If c is the nilpotent class of G and h is its class number, prove that $h \geq c|G|^{1/c} - c + 1$. Deduce that $|G| < e^{h-1}$ where e is the base of natural logarithms. [*Hint*: Let $Z_i = \zeta_i G$ and observe that $Z_{i+1} \backslash Z_i$ is the union of at least $|Z_{i+1} : Z_i| - 1$ conjugacy classes.]

16. If $G = \langle x_1, \ldots, x_n \rangle$, prove that $\gamma_i(G)$ is generated by all conjugates of the commutators $[x_{j_1}, \ldots, x_{j_i}]$ where $1 \leq j_r \leq n$. A group G is nilpotent of class $\leq c$ if and only if the identity $[x_1, x_2, \ldots, x_{c+1}] = 1$ holds in G.

5.2. Nilpotent Groups

We shall now embark on a more systematic study of nilpotent groups, beginning with some elementary facts which are used constantly.

5.2.1. *If G is a nilpotent group and $1 \neq N \lhd G$, then $N \cap \zeta G \neq 1$.*

Proof. Since $G = \zeta_c G$ for some c, there is a least positive integer i such that $N \cap \zeta_i G \neq 1$. Now$[N \cap \zeta_i G, G] \leq N \cap \zeta_{i-1} G = 1$ and $N \cap \zeta_i G \leq N \cap \zeta_1 G$. Hence $N \cap \zeta_1 G = N \cap \zeta_i G \neq 1$. □

5.2.2. *A minimal normal subgroup of a nilpotent group is contained in the center.*

This follows at once from 5.2.1.

5.2.3. *If A is a maximal normal abelian subgroup of the nilpotent group G, then $A = C_G(A)$.*

Proof. Of course $A \leq C = C_G(A)$ since A is abelian. Suppose that $A \neq C$: then C/A is a nontrivial normal subgroup of the nilpotent group G/A, and by 5.2.1 there is an element $xA \in (C/A) \cap \zeta(G/A)$ with $x \notin A$. Now $\langle x, A \rangle$ is abelian and it is normal in G because $\langle x, A \rangle/A \leq \zeta(G/A)$. Hence $x \in A$ by maximality of A. □

It should be observed that every group contains maximal normal abelian subgroups, not necessarily proper, by Zorn's Lemma. Lemma 5.2.3 indicates the degree to which such subgroups control a nilpotent group. For example, if A in 5.2.3 is finite, so is Aut A and therefore G/A since $A = C_G(A)$. Thus G is finite.

Characterizations of Finite Nilpotent Groups

There are several group-theoretical properties which for finite groups are equivalent to nilpotence. One of these is the *normalizer condition*, every proper subgroup is properly contained in its normalizer. Another such is the property that every maximal subgroup is normal. Here by a *maximal subgroup* we mean a *proper* subgroup which is not contained in any larger proper subgroup.

5.2.4. *Let G be a finite group. Then the following properties are equivalent*:

(i) *G is nilpotent*;
(ii) *every subgroup of G is subnormal*;
(iii) *G satisfies the normalizer condition*;
(iv) *every maximal subgroup of G is normal*;
(v) *G is the direct product of its Sylow subgroups.*

Proof. (i) → (ii). Let G be nilpotent with class c. If $H \leq G$, then $H\zeta_i G \lhd H\zeta_{i+1}G$ since $\zeta_{i+1}G/\zeta_i G = \zeta(G/\zeta_i G)$. Hence $H = H\zeta_0 G \lhd H\zeta_1 G \lhd \cdots \lhd H\zeta_c G = G$ and H is subnormal in G *in c steps*.

(ii) → (iii). Let $H < G$. Then H is subnormal in G and there is a series $H = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$. If i is the least positive integer such that $H \neq H_i$, then $H = H_{i-1} \lhd H_i$ and $H_i \leq N_G(H)$.

(iii) → (iv). If M is a maximal subgroup of G, then $M < N_G(M)$, so by maximality $N_G(M) = G$ and $M \lhd G$.

(iv) → (v). Let P be a Sylow subgroup of G. If P is not normal in G, then $N_G(P)$ is a proper subgroup of G and hence is contained in a maximal subgroup of G, say M. Then $M \lhd G$; however this contradicts 1.6.18. Therefore each Sylow subgroup of G is normal and there is exactly one Sylow p-subgroup for each prime p since all such are conjugate. The product of all the Sylow subgroups is clearly direct and it must equal G.

(v) → (i) by 5.1.3 and 5.1.4. □

For infinite groups the situation is much more complicated and properties (ii)–(v) are all weaker than nilpotency. We shall return to this topic in Chapter 12.

Tensor Products and Lower Central Factors

Our aim is to show that the first lower central factor $G_{\text{ab}} = G/G'$ exerts a very strong influence on subsequent lower central factors of a group G.

Let G be a group with operator domain Ω and write $G_i = \gamma_i G$; this is fully-invariant, so it is an Ω-admissible subgroup. Then G_i/G_{i+1}, being abelian, is a (right) Ω-module. We ask how the Ω-modules G_i/G_{i+1} are related to $G_{\text{ab}} = G_1/G_2$, the derived quotient group of G. (Keep in mind that these modules are being written multiplicatively.)

Let $g \in G$ and $a \in G_i$: consider the function $(aG_{i+1}, gG') \mapsto [a, g]G_{i+2}$. In the first place this is well-defined; for if $x \in G'$, then $[a, gx] = [a, x][a, g]^x \equiv [a, g] \bmod G_{i+2}$ since $[G_i, G'] \leq G_{i+2}$ by 5.1.11; in addition $[ay, g] = [a, g]^y[y, g] \equiv [a, g] \bmod G_{i+2}$ if $y \in G_{i+1}$. Our function is also bilinear; for $[a_1 a_2, g] = [a_1, g][a_1, g, a_2][a_2, g]$, whence $[a_1 a_2, g] \equiv [a_1, g][a_2, g] \bmod G_{i+2}$ since $[a_1, g, a_2] \in G_{i+2}$. Similarly $[a, g_1 g_2] \equiv [a, g_1][a, g_2] \bmod G_{i+2}$ since $[a, g_1, g_2] \in G_{i+2}$. By the fundamental mapping property of the tensor product (over $\mathbb{Z}$) there is an induced homomorphism

$$\varepsilon_i\colon (G_i/G_{i+1}) \otimes G_{ab} \to G_{i+1}/G_{i+2}$$

in which $(aG_{i+1}) \otimes (gG') \mapsto [a, g]G_{i+2}$. Since $G_{i+1} = [G_i, G]$, this is an epimorphism.

Now the lower central factors G_i/G_{i+1} are right Ω-modules and there is a natural way to make the tensor product $A \otimes B$ of two such modules A and B into an Ω-module, namely by diagonal action: $(a \otimes b)^\omega = a^\omega \otimes b^\omega$ ($a \in A$, $b \in B$, $\omega \in \Omega$). We check that ε_i is a homomorphism of Ω-modules:

$$(aG_{i+1} \otimes gG')^{\omega\varepsilon_i} = (a^\omega G_{i+1} \otimes g^\omega G')^{\varepsilon_i} = [a^\omega, g^\omega]G_{i+3} = ([a, g]G_{i+2})^\omega$$
$$= (aG_{i+1} \otimes gG')^{\varepsilon_i \omega}.$$

Our conclusions are summed up in the following result.

5.2.5 (Robinson). *Let G be an Ω-operator group and let $F_i = \gamma_i G/\gamma_{i+1} G$. Then the mapping $a(\gamma_{i+1} G) \otimes gG' \mapsto [a, g](\gamma_{i+2} G)$ is a well-defined Ω-epimorphism from $F_i \otimes_{\mathbb{Z}} G_{\text{ab}}$ to F_{i+1}.*

Iterating this result, we conclude that there is Ω-epimorphism from

$$\underbrace{G_{\text{ab}} \otimes \cdots \otimes G_{\text{ab}}}_{i}$$

to F_i. One would therefore expect G_{ab} to affect greatly the structure of subsequent lower central factors, and even the structure of G should it be nilpotent.

5.2.6. *Let $\mathscr{P}$ be a group-theoretical property which is inherited by images of tensor products and by extensions. If G is a nilpotent group such that G_{ab} has $\mathscr{P}$, then G has $\mathscr{P}$.*

Proof. Let $F_i = \gamma_i G/\gamma_{i+1} G$. Suppose F_i has $\mathscr{P}$; then F_{i+1}, being an image of $F_i \otimes G_{ab}$, has $\mathscr{P}$, whence every lower central factor has $\mathscr{P}$. But some $\gamma_{c+1} G = 1$ because G is nilpotent. Since $\mathscr{P}$ is closed under forming extensions, G has $\mathscr{P}$. □

For example, let $\mathscr{P}$ be the property of being finite. Then we obtain the result: *if G is a nilpotent group and G_{ab} is finite, then G too is finite.*

The Torsion-Subgroup of a Nilpotent Group

If π is a nonempty set of primes, a *π-number* is a positive integer whose prime divisors belong to π. An element of a group is called a *π-element* if its order is a π-number, and should every element be a π-element, the group is called a *π-group*. The most important case is $\pi = \{p\}$, when we speak of *p-elements* and *p-groups*. Observe that every element of a finite group is a p-element if and only if the group order is a power of p—by Sylow's Theorem. Hence for finite groups this usage of the term "p-group" is consistent with that employed in Chapter 1.

It should be borne in mind that infinite p-groups can easily have trivial center and therefore need not be nilpotent—see Exercise 5.2.11.

5.2.7. *Let G be a nilpotent group. Then the elements of finite order in G form a fully-invariant subgroup T such that G/T is torsion-free and $T = \mathrm{Dr}_p\, T_p$ where T_p is the unique maximum p-subgroup of G.*

Proof. Let π be a nonempty set of primes and let T_π denote the subgroup *generated* by all π-elements of G. Now $(T_\pi)_{ab}$ too is generated by π-elements and, being abelian, it is certainly a π-group. By 5.2.6 with $\mathscr{P}$ the property of being a π-group, the subgroup T_π is a π-group. Taking π to be the set of all primes we conclude that $T = T_\pi$ *consists* of elements of finite order, so T is torsion. Taking $\pi = \{p\}$, we see that T_p is a p-group. Clearly $T_p \lhd G$ and $T = \mathrm{Dr}_p\, T_p$. Obviously G/T must be torsion-free. □

The subgroup T of 5.2.7 is called the *torsion-subgroup* of G.

Products of Normal Nilpotent Subgroups

In the theory of groups a fundamental role is played by the next result.

5.2.8 (Fitting's Theorem). *Let M and N be normal nilpotent subgroups of a group G. If c and d are the nilpotent classes of M and N, then $L = MN$ is nilpotent of class at most $c + d$.*

Proof. We shall calculate the terms of the lower central series of L, showing by induction on i that $\gamma_i L$ is the product of all $[X_1, \dots, X_i]$ with $X_j = M$ or N, a statement which is correct for $i = 1$ if $[X_1] \equiv X_1$. The fundamental commutator identities show that

$$[UV, W] = [U, W][V, W] \qquad \text{and} \qquad [U, VW] = [U, V][U, W]$$

if $U, V, W \lhd G$. It follows that

$$\gamma_{i+1}L = [\gamma_i L, L] = [\gamma_i L, M][\gamma_i L, N]$$

and hence that $\gamma_{i+1}L$ is the product of all $[X_1, \dots, X_i, X_{i+1}]$ with $X_j = M$ or N.

To complete the proof set $i = c + d + 1$. Then in $[X_1, \dots, X_i]$ either M occurs at least $c + 1$ times or N occurs at least $d + 1$ times. Now $A \lhd G$ always implies that $[A, G] \leq A$ since $[a, g] = a^{-1}a^g$. Thus $[X_1, \dots, X_i]$ is contained in either $\gamma_{c+1}M$ or $\gamma_{d+1}N$, both of which equal 1. Consequently $[X_1, \dots, X_i] = 1$ and $\gamma_i L = 1$, so that L is nilpotent with class at most $i - 1 = c + d$. □

The Fitting Subgroup

The subgroup generated by all the normal nilpotent subgroups of a group G is called the *Fitting subgroup* of G and will be written

$$\text{Fit } G.$$

If the group G is finite (or just satisfies max-n), Fit G is nilpotent, and evidently it is the unique largest normal nilpotent subgroup of G. Of course Fit G may be trivial—the finite groups with this property are precisely the semisimple groups of 3.3. On the other hand, if G is a nontrivial soluble group, Fit G contains the smallest nontrivial term of the derived series and hence cannot be 1.

For finite groups there is another interpretation of the Fitting subgroup. To describe this we need to generalize the notion of a centralizer. Let G be a group with operator domain Ω and let $X \subseteq G$; define the *centralizer of X in Ω* to be $C_\Omega(X) = \{\omega \in \Omega \mid x^\omega = x, \forall x \in X\}$. This enables us to speak of the centralizer in G of a principal factor.

5.2.9. *If G is a finite group, then* Fit G *is the intersection of the centralizers of the principal factors of G.*

Proof. Let $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ be a principal series of G and let I be the intersection of all the $C_G(G_{i+1}/G_i)$. Then $[G_{i+1}, I] \leq G_i$ for all i, whence $\gamma_{n+1}I = 1$ and I is nilpotent: clearly $I \lhd G$, so $I \leq F = \text{Fit } G$. Conversely, we have $[G_1, F] \lhd G$ and $[G_1, F] \leq G_1$. Since G_1 is a minimal normal subgroup of G, either $[G_1, F] = 1$ or $[G_1, F] = G_1$: in the latter event repeated commutation with F yields $G_1 \leq \gamma_{c+1}F = 1$ for some c, a contradiction. Hence F must centralizes G_1. If $n > 1$, induction on n shows that FG_1/G_1, and hence F, centralizes G_{i+1}/G_i if $i \geq 1$. □

P. Hall's Criterion for Nilpotence

An extension of one nilpotent group by another need not be nilpotent—as S_3 shows. Thus one cannot prove Fitting's Theorem as simply as 5.1.2. There is, however, an important criterion for such an extension to be nilpotent.

5.2.10 (P. Hall). *If $N \lhd G$ and N and G/N' are nilpotent, then G is nilpotent.*

Proof. Let N and G/N' have respective nilpotent classes c and d. Regard N_{ab} as a group with operator domain G, the elements of G acting by conjugation. Since G/N' is nilpotent, a central series of G/N' can be intersected with N_{ab} to produce a G-series of N_{ab} whose factors are *trivial G-modules*, that is, each element of G acts like the identity automorphism. Let us call a G-module having a series with G-trivial factors *polytrivial*. Let $F_i = \gamma_i N/\gamma_{i+1}N$; then $F_1 = N_{ab}$ is polytrivial. Suppose that F_i is polytrivial. Since F_{i+1} is an image of $F_i \otimes N_{ab}$, should we be able to prove that the tensor product of two polytrivial G-modules is polytrivial, it will follow that F_{i+1} is polytrivial. Therefore every lower central factor of N will be a polytrivial G-module. If we form the preimage of each term of a series of F_i with G-trivial factors under the canonical homomorphism $\gamma_i N \to F_i$ and also preimages of terms of a central series of G/N under the canonical homomorphism $G \to G/N$, we shall obtain a central series of G and G will be nilpotent.

All that remains, then, is to establish the following result.

5.2.11. *Let A and B be polytrivial G-modules where G is any group. Then $A \otimes_{\mathbb{Z}} B$ is a polytrivial G-module.*

Proof. By hypothesis there exist G-series $0 = A_0 < A_1 < \cdots A_r = A$ and $0 = B_0 < B_1 < \cdots < B_s = B$ such that A_{j+1}/A_j and B_{k+1}/B_k are trivial G-modules. We define a series in $T = A \otimes_{\mathbb{Z}} B$ as follows: let T_i be generated by all $a \otimes b$ where $a \in A_j$, $b \in B_k$ and $j + k \leq i$. Then $0 = T_0 = T_1 \leq T_2 \leq \cdots \leq T_{r+s} = T$. Let $g \in G$, $a \in A_{j+1}$ and $b \in B_{k+1}$: then $ag = a + a'$ and $bg = b + b'$ where $a' \in A_j$ and $b' \in B_k$. Hence $(a \otimes b)g = (a + a') \otimes (b + b') = a \otimes b + a \otimes b' + a' \otimes b + a' \otimes b'$ and $(a \otimes b)g \equiv a \otimes b \bmod T_{j+k+1}$. It follows that each T_i is a G-module and that T_{j+k+2}/T_{j+k+1} is a trivial G-module. Hence T is polytrivial. □

The Frattini† Subgroup

The Frattini subgroup of an arbitrary group G is defined to be the intersection of all the maximal subgroups, with the stipulation that it shall equal G if G should prove to have no maximal subgroups. This subgroup, which is evidently characteristic, is written

$$\text{Frat } G.$$

The Frattini subgroup has the remarkable property that it is the set of all nongenerators of the group; here an element g is called a *nongenerator* of G if $G = \langle g, X \rangle$ always implies that $G = \langle X \rangle$ when X is a subset of G.

5.2.12 (Frattini). *In any group G the Frattini subgroup equals the set of nongenerators of G.*

Proof. Let $g \in \text{Frat } G$ and suppose that $G = \langle g, X \rangle$ but $G \neq \langle X \rangle$. Then $g \notin \langle X \rangle$, so by 3.3.14 there exists a subgroup M which is maximal subject to $\langle X \rangle \leq M$ and $g \notin M$. Now if $M < H \leq G$, then $g \in H$ and $H = G$. Consequently M is maximal in G. But $g \in \text{Frat } G \leq M$ and consequently $G = \langle g, X \rangle = M$, a contradiction. Hence g is a nongenerator.

Conversely suppose that g is a nonegnerator which does not belong to $\text{Frat } G$, so that $g \notin M$ for some maximal subgroup M of G. Then $M \neq \langle g, M \rangle$, whence $G = \langle g, M \rangle$. But this implies that $G = M$ since g is a nongenerator. □

We collect together next a number of elementary properties of the Frattini subgroup of a finite group.

5.2.13. *Let G be a finite group.*

(i) *If $N \lhd G$, $H \leq G$ and $N \leq \text{Frat } H$, then $N \leq \text{Frat } G$.*
(ii) *If $K \lhd G$, then $\text{Frat } K \leq \text{Frat } G$.*
(iii) *If $N \lhd G$, then $\text{Frat}(G/N) \geq (\text{Frat } G)N/N$ with equality if $N \leq \text{Frat } G$.*
(iv) *If A is an abelian normal subgroup of G such that $(\text{Frat } G) \cap A = 1$, there is a subgroup H such that $G = HA$ and $H \cap A = 1$.*

Proof. (i) If $N \nleq \text{Frat } G$, then $N \nleq M$ for some maximal subgroup M and $G = MN$. Hence $H = H \cap (MN) = (H \cap M)N$. By 5.2.12 it follows that $H = H \cap M$ and $H \leq M$; but this gives the contradiction $N \leq M$.

(ii) Apply (i) with $N = \text{Frat } K$ and $H = K$.

(iii) This follows at once from the definition.

(iv) Choose $H \leq G$ minimal subject to $G = HA$. Now $H \cap A \lhd H$ and also $H \cap A \lhd A$ since A is abelian: therefore $H \cap A \lhd HA = G$. If $H \cap A \leq$

† Giovanni Frattini (1852–1925).

Frat H, then (i) shows that $H \cap A \leq (\text{Frat } G) \cap A = 1$. Thus we can assume that $H \cap A \nleq M$ for some M maximal in H, in which case $H = M(H \cap A)$ and $G = HA = MA$, in contradiction to the minimality of H. □

5.2.14. *If H is a finite normal subgroup of a group G and P is a Sylow p-subgroup of H, then $G = N_G(P)H$.*

Proof. Let $g \in G$; then $P^g \leq H$ and P^g is Sylow p-subgroup of H. Hence $P^g = P^h$ for some $h \in H$ by Sylow's Theorem. Consequently $gh^{-1} \in N_G(P)$ and $g \in N_G(P)H$ as required. □

The proof of this enormously useful result is usually referred to as *the Frattini argument.* One application is to show that the Frattini subgroup of a finite group is nilpotent, a fact first established by Frattini himself. Indeed, a good deal more can be proved.

5.2.15 (Gaschütz). *Let G be a group.*

(i) *If* Frat $G \leq H \lhd G$ *where H is finite and $H/$*Frat G *is nilpotent, then H is nilpotent. In particular* Frat G *is always nilpotent if it is finite.*
(ii) *Let* FFrat G *be defined by* FFrat $G/$Frat G = Fit($G/$Frat G). *If G is finite, then* FFrat G = Fit G; *also* FFrat $G/$Frat G *is the product of all the abelian minimal normal subgroups of* $G/$Frat G.

Proof. (i) Let P be a Sylow p-subgroup of H; by 5.2.4 it is enough to prove that $P \lhd G$. Let $F = \text{Frat } G$ and $K = PF \leq H$. Since K/F is a Sylow p-subgroup of H/F (by 1.6.18) and H/F is nilpotent, K/F is characteristic in H/F, whence $K \lhd G$. Now apply 5.2.14 to conclude that $G = N_G(P)K = N_G(P)F$, which shows that $G = N_G(P)$ and $P \lhd G$.

(ii) Taking H to be FFrat G in (i) we deduce that H is nilpotent and $H \leq \text{Fit } G$. But the opposite inclusion is obviously true, so $H = \text{Fit } G$.

In the final part we can assume that Frat $G = 1$. Write $L = \text{Fit } G$. By 5.2.4 a maximal subgroup of L is normal and has prime index. Hence $L' \leq \text{Frat } L \leq \text{Frat } G = 1$ and L is abelian. Denote by N the product of all the abelian minimal normal subgroups of G; then certainly $N \leq L$. By 5.2.13 there exists a subgroup H such that $G = HN$ and $H \cap N = 1$. Now $H \cap L \lhd H$ and $H \cap L \lhd L$ since L is abelian. Thus $H \cap L \lhd HL = G$. Since $(H \cap L) \cap N = 1$, the normal subgroup $H \cap L$ cannot contain a minimal normal subgroup of G; we conclude that $H \cap L = 1$ and $L = L \cap (HN) = N$. □

We turn now to the Frattini subgroups of nilpotent groups. Observe that if a maximal subgroup M of a group G is normal, then G/M has prime order and $G' \leq M$. Thus $M \lhd G$ if and only if $G' \leq M$. All maximal subgroups of G are normal if and only if $G' \leq \text{Frat } G$. The following result is therefore an immediate consequence of 5.2.4.

5.2.16 (Wielandt). *Let G be a finite group. Then G is nilpotent if and only if $G' \leq \operatorname{Frat} G$.*

Finitely Generated Nilpotent Groups

We have seen in 4.2.8 that finitely generated abelian groups satisfy the maximal condition. In fact this result may be generalized to nilpotent groups on the basis of the following theorem.

5.2.17 (Baer). *If G is a nilpotent group and G_{ab} is finitely generated, then G satisfies the maximal condition.*

Proof. The tensor product of two finitely generated abelian groups is clearly finitely generated. Therefore by 5.2.5 each lower central factor of G is finitely generated. It follows that such factors satisfy max. The theorem is now a consequence of 3.1.7. □

5.2.18. *A finitely generated nilpotent group has a central series whose factors are cyclic groups with prime or infinite orders.*

Proof. Use 5.2.17 and refine the lower central series suitably. □

From this it is obvious that *a finitely generated nilpotent torsion group is finite.* Of particular interest are finitely generated torsion-free nilpotent groups, of which the unitriangular group $U(n, \mathbb{Z})$ is an example.

5.2.19 (Mal'cev†). *If the center of a group G is torsion-free, each upper central factor is torsion-free.*

Proof. Let $\zeta G = \zeta_1 G$ be torsion-free; it is enough to prove that $\zeta_2 G/\zeta_1 G$ is torsion-free. Suppose that $x \in \zeta_2 G$ and $x^m \in \zeta_1 G$ where $m > 0$. By Exercise 5.1.4 we have $[x, g]^m = [x^m, g] = 1$ because $[x, g] \in \zeta_1 G$. Since $\zeta_1 G$ is torsion-free, $[x, g] = 1$ for all $g \in G$, and $x \in \zeta_1 G$. □

5.2.20. *A finitely generated torsion-free nilpotent group has a central series with infinite cyclic factors.*

Proof. The upper central factors are torsion-free by 5.2.19 and finitely generated by 5.2.17; hence they are free abelian groups with finite rank. On refining this series we obtain one of the required type. □

The next theorem exhibits a surprising connection between finitely generated torsion-free nilpotent groups and finite p-groups, namely that the former are very rich in finite p-images.

† Anatoliĭ Ivanovič Mal'cev (1909–1967).

5.2.21 (Gruenberg). *A finitely generated torsion-free nilpotent group G is a residually finite p-group for every prime p.*

In order to prove this we need a further result.

5.2.22. *Let G be a nilpotent group.*

(i) *If ζG has exponent e, then G has exponent dividing e^c where c is the class of G.*
(ii) *If G is finitely generated and infinite, then ζG contains an element of infinite order.*

Proof. (i) Assume that $G \neq \zeta G$. Let $x \in \zeta_2 G$ and $g \in G$. Then $[x, g] \in \zeta G$ and $1 = [x, g]^e = [x^e, g]$, whence $x^e \in \zeta_1 G$. Thus $\zeta_2 G/\zeta_1 G$ has finite exponent dividing e. By induction $G/\zeta_1 G$ has exponent dividing e^{c-1} and G has exponent dividing e^c.

(ii) If ζG is a torsion group, it is finite by 5.2.17 and 4.2.9. By (i) the group G is a torsion group, whence it is finite by 5.2.18. □

Proof of **5.2.21.** Let $G \neq 1$ and put $C = \zeta G$. By 5.2.19 the group G/C is torsion-free and we can apply induction on the nilpotent class to show that this is a residually finite p-group. Let $1 \neq g \in G$; we have to find a normal subgroup not containing g which has index a power of p. If $g \notin C$, then $gC \neq 1_{G/C}$ and all is well by virtue of the residual property of G/C. Assume therefore that $g \in C$.

Since C is free abelian, $\bigcap_{i=1,2,\ldots} C^{p^i} = 1$ and $g \notin L = C^{p^i}$ for some i. Choose $N \lhd G$ maximal subject to $L \leq N$ and $g \notin N$, using max (or 3.3.14). If G/N is infinite, 5.2.22 shows that its center contains an element zN of infinite order. Since $\langle z, N\rangle \lhd G$, maximality of N yields $g \in \langle z, N\rangle$ and $g \equiv z^r \bmod N$ for some $r \neq 0$. But then $z^r \in CN$, and, C/L being finite, $z^s \in LN = N$ for some $s > 0$. This is impossible since zN has infinite order. Therefore G/N is finite.

Next $L \leq C \cap N < C$, so $|CN : N| \neq 1$ divides $|C : L|$, which is surely a power of p. It follows that the Sylow p-subgroup P/N of G/N is nontrivial. If for some $q \neq p$ the Sylow q-subgroup Q/N were also nontrivial, we should have $g \in P \cap Q = N$ by maximality of N. Hence G/N is a finite p-group. □

Exercises 5.2

1. If a nilpotent group has an element of prime order p, so does it center.

*2. Let A be a nontrivial abelian group and set $D = A \times A$. Define $\delta \in \operatorname{Aut} D$ as follows: $(a_1, a_2)^\delta = (a_1, a_1 a_2)$. Let G be the semidirect product $\langle \delta \rangle \ltimes D$.
   (a) Prove that G is nilpotent of class 2 and $\zeta G = G' \simeq A$.
   (b) Prove that G is a torsion group if and only if A has finite exponent.
   (c) Deduce that even if the center of a nilpotent group is a torsion group, the group may contain elements of infinite order (cf. 5.2.22 (i)).

3. If M and N are nontrivial normal nilpotent subgroups of a group, prove from first principles that $\zeta(MN) \neq 1$. Hence give an alternative proof of Fitting's Theorem for finite groups.
4. The Fitting subgroup of an infinite group need not be nilpotent.
5. Let H and K be quasicyclic groups and write $G = H \wr K$ for the standard wreath product. Prove that $G = \text{Frat } G$ and deduce that the Frattini subgroup is not always nilpotent.
6. A nontrivial finitely generated group cannot equal its Frattini subgroup.
7. Let $G_i = \zeta_i G$ and $F_i = G_{i+1}/G_i$ where G is an arbitrary group. Show that there is a monomorphism $F_{i+1} \to \text{Hom}(G_{ab}, F_i)$.
8. Find an upper bound for the nilpotent class in Hall's criterion 5.2.10. (See also [a199].)
9. Prove that $\text{Frat}(S_n) = 1$.
10. Find $\text{Frat}(D_{2n})$ and $\text{Frat}(D_\infty)$.

*11. There exist infinite soluble p-groups with trivial center. [*Hint*: Consider the standard wreath product $\mathbb{Z}_p \wr E$ where E is an infinite elementary abelian p-group.]

*12. If $G = \text{Dr}_p\, G_p$ where G_p is a p-group and if $H \leq G$, prove that $H = \text{Dr}_p(H \cap G_p)$.

13. Let G be a torsion-free nilpotent group and let H be a subgroup with finite index. Prove that G and H have the same nilpotent class.
14. Let G be a finitely generated group. Prove that G has a unique maximal subgroup if and only if G is a nontrivial cyclic p-group for some prime. Also give an example of a noncyclic abelian p-group with a unique maximal subgroup.

5.3. Groups of Prime-Power Order

Finite p-groups occupy a central position in the theory of groups. Since their structure can be extremely complex, we shall largely limit ourselves to the investigation of special types. Firstly some elementary facts about finite p-groups in general.

5.3.1. *Let G be a group of order p^{m+1} where p is a prime.*

(i) *If G has nilpotent class $c > 1$, then $G/\zeta_{c-1}G$ is not cyclic, so its order is at least p^2. Moreover $c \leq m$.*
(ii) *If $0 \leq i \leq j \leq m+1$, every subgroup of order p^i is contained in some subgroup of order p^j. In particular there are subgroups of every order dividing p^{m+1}.*

Proof. (i) If $G/\zeta_{c-1}G$ were cyclic, then $G/\zeta_{c-2}G$ would be abelian, which implies that $\zeta_{c-1}G = G$ and the class of G is less than c.

(ii) Let H be a subgroup of order p^i. Since H is subnormal in G, it is a term of a composition series of G. Some term of this series will have order p^j since all composition factors are of order p. □

5.3.2 (The Burnside Basis Theorem). *Let G be a finite p-group. Then* Frat $G = G'G^p$. *Also, if* $|G : \text{Frat } G| = p^r$, *every set of generators of G has a subset of r elements which also generates G.*

Proof. If M is maximal in G, we know from 5.2.4 that $M \lhd G$ and $|G : M| = p$. Hence $G'G^p \leq \text{Frat } G$. On the other hand $G/G'G^p$ is an elementary abelian p-group and such groups have trivial Frattini subgroup. Therefore Frat $G = G'G^p$.

Now let $G = \langle x_1, \ldots, x_s \rangle$ and put $F = \text{Frat } G$. Then $\bar{G} = G/F$ is generated by $x_1F, \ldots, x_sF$. Since $\bar{G}$ is a vector space of dimension r over $GF(p)$, it has a basis of the form $\{x_{i_1}F, \ldots, x_{i_r}F\}$. Writing $Y = \langle x_{i_1}, \ldots, x_{i_r} \rangle$, we have $G = \langle Y, F \rangle$ and hence $G = \langle Y \rangle$. □

Let us use the Burnside Basis Theorem to obtain information about the automorphism group of a finite p-group.

5.3.3 (P. Hall). *Let G be a group of order p^m and let* $|G : \text{Frat } G| = p^r$. *Then the order of* $C_{\text{Aut } G}(G/\text{Frat } G)$ *divides* $p^{(m-r)r}$ *and the order of* Aut G *divides* $np^{(m-r)r}$ *where* $n = |\text{GL}(r, p)|$.

Proof. Write $F = \text{Frat } G$ and $C = C_{\text{Aut } G}(G/F)$. Then $(\text{Aut } G)/C$ is isomorphic with a subgroup of $\text{GL}(r, p)$ since G/F is a vector space of dimension r over $\text{GF}(p)$; thus $|(\text{Aut } G) : C|$ divides n. By 5.3.2. there exist generators $x_1, \ldots, x_r$ for G. Let us write $\mathbf{x} = (x_1, \ldots, x_r)$ for the *ordered* set of r generators. If $f_i \in F$ and $y_i = x_i f_i$, then $\mathbf{y} = (y_1, \ldots, y_r)$ is also an ordered set of r generators of G because $G = \langle y_1, \ldots, y_r, F \rangle$ implies that $G = \langle y_1, \ldots, y_r \rangle$. The set $\mathbf{S}$ of all ordered sets of r generators obtainable from $\mathbf{x}$ in this manner has exactly $|F|^r = p^{(m-r)r}$ elements. If $\gamma \in C$ and $\mathbf{y} \in \mathbf{S}$, define $\mathbf{y}^\gamma$ to be $(y_1^\gamma, \ldots, y_r^\gamma)$; since $y_i^\gamma \equiv y_i \bmod F$, in fact $\mathbf{y}^\gamma \in \mathbf{S}$. The function $\mathbf{y} \mapsto \mathbf{y}^\gamma$ is a permutation of $\mathbf{S}$, so we have an action of C on $\mathbf{S}$. If $\mathbf{y}^\gamma = \mathbf{y}$, then $y_i^\gamma = y_i$ for all i, and since the y_i's generate G, it follows that $\gamma = 1$. Thus each $\mathbf{y}$ in $\mathbf{S}$ is fixed only by 1 in C, so that C acts semiregularly on $\mathbf{S}$. Consequently each orbit has $c = |C|$ elements. If l is the number of orbits, then $cl = p^{(m-r)r}$ and c divides $p^{(m-r)r}$. Finally $|\text{Aut } G| = |(\text{Aut } G) : C| \cdot |C|$, which divides $np^{(m-r)r}$. □

Quaternion Groups

An important type of finite 2-group that occurs in many investigations is the *generalized quaternion group* Q_{2^n}, $(n \geq 3)$; this is a group with a presenta-

tion of the form

$$\langle x, y | x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, y^{-1}xy = x^{-1}\rangle.$$

This group may be realized in the following manner. Let $\langle \bar{u} \rangle$ and $\langle \bar{v} \rangle$ be cyclic groups of order 2^{n-1} and ∞ respectively and let $G = \langle \bar{v} \rangle \ltimes \langle \bar{u} \rangle$ be the semidirect product where $\bar{v}$ induces the automorphism $a \mapsto a^{-1}$ in $\langle \bar{u} \rangle$. Let $\bar{w} = \bar{u}^{2^{n-2}}\bar{v}^{-2}$: then $\bar{w}^{\bar{u}} = \bar{w} = \bar{w}^{\bar{v}}$, so that $\bar{w} \in \zeta G$ and $\langle \bar{w} \rangle \lhd G$. Now put $Q = G/\langle \bar{w} \rangle$ and write $u = \bar{u}\langle \bar{w} \rangle$ and $v = \bar{v}\langle \bar{w} \rangle$; then $u^{2^{n-1}} = 1$, $v^2 = u^{2^{n-2}}$ and $v^{-1}uv = u^{-1}$. By von Dyck's theorem (2.2.1) there is an epimorphism from Q_{2^n} to Q in which $x \mapsto u$ and $y \mapsto v$. Now what is the order of Q? In the first place $\langle \bar{u} \rangle \cap \langle \bar{w} \rangle = 1$ (proof?), so $u = \bar{u}\langle \bar{w} \rangle$ has order 2^{n-1}. Also $v^2 \in \langle u \rangle$, while $v \in \langle u \rangle$ would imply that $\bar{v} = \bar{u}^i\bar{w}^j = \bar{u}^{i+j2^{n-2}}\bar{v}^{-2j}$ and $\bar{v}^{1+2j} = \bar{u}^{i+j2^{n-2}}$ for some i and j, which is impossible. Thus $|Q : \langle u \rangle| = 2$ and $|Q| = 2^n$. But we see at once from the presentation that $|Q_{2^n}|$ divides 2^n. Thus $Q \simeq Q_{2^n}$ and Q_{2^n} has order 2^n.

The group Q_8, which has order 8, is best known as the group of *Hamilton's*† *quaternions*: this is the group consisting of the symbols ± 1, $\pm i$, $\pm j$, $\pm k$ where $-1 = i^2 = j^2 = k^2$ and $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$ (see Exercise 5.3.1).

Some Special Types of Finite p-Groups

As our first major result on p-groups we shall classify finite p-groups which have a cyclic maximal subgroup.

5.3.4. *A group of order p^n has a cyclic maximal subgroup if and only if it is of one of the following types*:

(i) *a cyclic group of order p^n*;
(ii) *the direct product of a cyclic group of order p^{n-1} and one of order p*;
(iii) $\langle x, a | x^p = 1 = a^{p^{n-1}}, a^x = a^{1+p^{n-2}}\rangle$, $n \geq 3$;
(iv) *the dihedral group D_{2^n}, $n \geq 3$*;
(v) *the generalized quaternion group Q_{2^n}, $n \geq 3$*;
(vi) *the semidihedral group $\langle x, a | x^2 = 1 = a^{2^{n-1}}, a^x = a^{2^{n-2}-1}\rangle$, $n \geq 3$.*

We shall need here and elsewhere the following elementary fact.

5.3.5. *In a nilpotent group of class at most 2 the identity $(xy)^m = x^m y^m [y, x]^{\binom{m}{2}}$ holds.*

Proof. The result is obviously true when $m = 1$: proceed by induction on m. Using the induction hypothesis and the fact that $[x, y]$ lies in the center, we obtain that $(xy)^{m+1} = x^m(y^m x)y[y, x]^{\binom{m}{2}}$. Now Exercise 5.1.4 shows that

† Sir William Rowan Hamilton (1805–1865).

$[y^m, x] = [y, x]^m$. Hence $y^m x = xy^m[y, x]^m$ and therefore

$$(xy)^{m+1} = x^{m+1}y^{m+1}[y, x]^{\binom{m+1}{2}}$$

since $\binom{m+1}{2} = \binom{m}{2} + m$. □

***Proof of* 5.3.4.** Let $|G| = p^n$. Suppose that $N = \langle a \rangle$ is a cyclic maximal subgroup: then $N \lhd G$ and $|G : N| = p$. Writing $G/N = \langle xN \rangle$, we have $G = \langle x, a \rangle$: also $|a| = p^{n-1}$ and $x^p \in N$. If G is abelian and $x^p = b^p$ where $b \in N$, then $(xb^{-1})^p = 1$ and $G = \langle xb^{-1} \rangle \times N$; otherwise $x^p = a^i$ where $(i, p) = 1$, and $G = \langle x \rangle$. Thus, if G is abelian, it is of type (i) or (ii). Henceforth we shall assume that G is not abelian, so that $n > 2$.

The element x induces an automorphism in N which must have order p: hence $a^x = a^m$ where $m^p \equiv 1 \bmod p^{n-1}$ and $1 < m < p^{n-1}$. Now by Fermat's Theorem $m^{p-1} \equiv 1 \bmod p$, so it follows that $m \equiv 1 \bmod p$.

For the moment assume that p is odd. Write $m = 1 + kp^i$ where $(p, k) = 1$ and, of course, $0 < i < n - 1$. Now

$$m^p = (1 + kp^i)^p = 1 + kp^{i+1} + \frac{p-1}{2}k^2p^{2i+1} + \frac{(p-1)(p-2)}{6}k^3p^{3i+1} + \cdots,$$

which shows that $m^p \equiv 1 + kp^{i+1} \bmod p^{i+2}$. But $m^p \equiv 1 \bmod p^{n-1}$, so that $kp^{i+1} + lp^{i+2} = l'p^{n-1}$ with integral l and l'. Since $i + 1 \leq n - 1$ and $(p, k) = 1$, it follows that $i + 1 = n - 1$ and $i = n - 2$. Thus $m = 1 + kp^{n-2}$: now there exists a k' such that $kk' \equiv 1 \bmod p$ and $a^{x^{k'}} = a^{(1+kp^{n-2})^{k'}} = a^{1+p^{n-2}}$, indicating that we may replace x by $x^{k'}$ and assume that $m = 1 + p^{n-2}$. It remains to discuss the position of x^p in N. Now $(x^p)^x = x^p$ implies that $|x^p|$ divides p^{n-2} and $x^p \in \langle a^p \rangle$, say $x^p = b^p$ where $b \in N$. Also G is nilpotent of class 2 since $[a, x] = a^{p^{n-2}}$. Hence $(xb^{-1})^p = x^pb^{-p} = 1$ by 5.3.5 since $[b^{-1}, x]^p = 1$. Replacing x by xb^{-1}, we can assume that $x^p = 1$, so that G is of type (iii).

From now on let $p = 2$. Certainly m is odd, equal to $2k + 1$ say. From $m^2 \equiv 1 \bmod 2^{n-1}$, it follows that $k(k + 1) \equiv 0 \bmod 2^{n-3}$ and $k \equiv 0$ or $-1 \bmod 2^{n-3}$. There are, therefore, two possible forms: $m = 2^{n-2}l + 1$ where l is odd, and $m = 2^{n-2}l - 1$. In the first case, replacing x by a suitable power, we may assume that $m = 2^{n-2} + 1$, while in the second either l is even and $m = 2^{n-1} - 1$ or l is odd and we may take $m = 2^{n-2} - 1$. There are, therefore, three cases to examine.

Suppose that $m = 2^{n-1} - 1$, so that $a^x = a^{-1}$. Since $(x^2)^x = x^2$, the element x^2 has order 1 or 2 in N, which shows that $x^2 = 1$ or a^{2n-2} and $G \simeq D_{2^n}$ or Q_{2^n} respectively. Now assume that $m = 2^{n-2} + 1$. Since x^2 cannot generate N, we have $x^2 = a^{2r}$ for some r. Setting $b = a^{r(2^{n-3}-1)}$, we compute that $(xb)^2 = x^2b^2[b, x] = a^{2r}a^{r(2^{n-2}-2)}a^{r(2^{n-3}-1)2^{n-2}} = a^{r2^{2n-5}}$. If $n \geq 4$, this power of a equals 1 and G is of type (iii). However, if $n = 3$, then $a^x = a^{-1}$ and $x^2 = 1$ or a^2, so that $G \simeq D_8$ or Q_8.

Finally, let $m = 2^{n-2} - 1$. If $x^2 = a^{2r}$, then $a^{2r} = (a^{2r})^x = a^{2r(2^{n-2}-1)}$, in which event $2r \equiv 0 \bmod 2^{n-2}$ and $x^2 = 1$ or $a^{2^{n-2}}$. If $x^2 \neq 1$, then $(xa^{-1})^2 = a^{2^{n-2}}a^{-2}a^{-(2^{n-2}-2)} = 1$ and G is of type (vi). □

Finite p-Groups with a Single Subgroup of Order p

5.3.6. *A finite p-group has exactly one subgroup of order p if and only if it is cyclic or a generalized quaternion group.*

Proof. In the first place, cyclic p-groups and generalized quaternion groups have the property in question. Let G have order p^n and assume that there is just one subgroup of order p. If G is abelian, the structure of finite abelian groups (4.2.6) tells us that G must be cyclic. Assume therefore that G is not abelian. Suppose that p is odd and let H be a maximal subgroup of G. By induction H is cyclic and so G has a cyclic maximal subgroup. Examining the list of groups in 5.3.4 we see that none of them qualify. It follows that $p = 2$.

Let A be a maximal normal abelian subgroup of G. Then A must be cyclic, generated by a say. Also $A = C_G(A)$ by 5.2.3. Let xA be an element of G/A with order 2. Now $\langle x, A\rangle$ is not abelian and it has a cyclic subgroup of index 2, so by 5.3.4 it is a generalized quaternion group, all the other types having more than one subgroup of order 2. Hence $a^x = a^{-1}$, which establishes that G/A has just one element of order 2. Now G/A is isomorphic with a subgroup of Aut A and Aut $A \simeq \mathbb{Z}^*_{2^m}$ where $|A| = 2^m$ by 1.5.5. Hence G/A is abelian and therefore cyclic. But -1 is not a square modulo 2^m unless $m = 1$, which is forbidden since it would force A to lie in the center of G. Therefore G/A has order 2 and G is a generalized quaternion group. □

Groups in Which Every Subgroup Is Normal

In $Q = Q_8$, the quaternion group of order 8, there is only one element of order 2 and it generates Q'. Hence $1 \neq H \leq Q$ implies that $Q' \leq H$ and $H \lhd Q$. So every subgroup of Q is normal. Our aim is to classify all groups with this property: these are known as *Dedekind groups* (a nonabelian Dedekind group is called *Hamiltonian*). We shall find that they are not far removed from Q_8.

5.3.7 (Dedekind, Baer). *All the subgroups of a group G are normal if and only if G is abelian or the direct product of a quaternion group of order* 8, *an elementary abelian* 2-*group and an abelian group with all its elements of odd order.*

Proof. We assume that every subgroup of G is normal but G is not abelian. Let x and y be two noncommuting elements and put $c = [x, y]$. Since $\langle x\rangle \lhd$

G and $\langle y \rangle \lhd G$, we have $c \in \langle x \rangle \cap \langle y \rangle$ and therefore $x^r = c = y^s$ where r, $s \neq 0$ or 1. Writing $Q = \langle x, y \rangle$, we see that $c \in \zeta Q$ and $Q' = \langle c \rangle$; thus Q is nilpotent of class 2. Hence $c^r = [x, y]^r = [x^r, y] = [c, y] = 1$, which implies that c, x, and y have finite orders. Consequently Q is finite.

Let $|x| = m$ and $|y| = n$. We shall suppose x and y so chosen that $m + n$ is minimal subject to $c = [x, y] \neq 1$. If p is a prime divisor of m, the assumption of minimality implies that $1 = [x^p, y] = c^p$ and c has order p. This tells us that $|x|$ and $|y|$ are powers of p.

Since c is a power of x and of y, there exist integers k, l, r, s such that $x^{kp^r} = c = y^{lp^s}$ and $(k, p) = 1 = (l, p)$. Now there are integers k', l' such that $kk' \equiv 1 \bmod p$ and $ll' \equiv 1 \bmod p$. Setting $x' = x^{l'}$ and $y' = y^{k'}$, we have $[x', y'] = c^{k'l'}$; also $(x')^{p^r} = (x^{p^r})^{l'} = c^{k'l'}$ since $c^{k'} = x^{kk'p^r} = x^{p^r}$, and similarly $(y')^{p^s} = c^{k'l'}$. Thus, replacing x by x' and y by y', we may assume that

$$x^{p^r} = c = y^{p^s} \qquad (r, s > 0).$$

Evidently $|x| = p^{r+1}$ and $|y| = p^{s+1}$. Without loss of generality let $r \geq s$.

If y_1 denotes $x^{-p^{r-s}}y$, then $[x, y_1] = [x, y] = c$ and, by minimality of $|x| + |y|$, we must have $|y_1| \geq |y| = p^{s+1}$; hence $y_1^{p^s} \neq 1$. By 5.3.5 we have

$$y_1^{p^s} = x^{-p^r} y^{p^s} [y, x^{-p^{r-s}}]^{\binom{p^s}{2}} = c^{-p^r(p^s-1)/2}.$$

If p is odd, it divides $-\frac{1}{2}p^r(p^s - 1)$ and $y_1^{p^s} = 1$. Therefore $p = 2$ and $2^{r-1}(2^s - 1)$ is odd, that is, $r = 1$. Since $r \geq s$, we have also $s = 1$. The following relations are therefore vaid, $x^4 = 1$, $x^2 = y^2$ and $x^y = x^{-1}$. Consequently $Q = \langle x, y \rangle$ is an image of a quaternion group of order 8. Since Q is not abelian, it *is* a quaternion group of order 8.

Next consider $C = C_G(Q)$ and suppose that $g \in G \backslash CQ$. Then g does not commute with both x and y—say $y^g \neq y$. Since $|y| = 4$, we must have $y^g = y^{-1}$; therefore gx commutes with y. Thus gx cannot commute with x (or else $gx \in C$). The same argument shows that gxy commutes with x: but clearly gxy also commutes with y. so $gxy \in C$ and $g \in CQ$. It follows that $G = CQ$. If $g \in C$, then $[x, gy] = [x, y] \neq 1$ and by the first paragraph of the proof gy has finite order. Since g and y commute, g has finite order and G is a torsion group. Next suppose that g in C has order 4. Then $[x, gy] \neq 1$ and $(gy)^4 = 1$, which implies that $(gy)^x = (gy)^{-1}$. Thus $[gy, x] = (gy)^{-2} = g^{-2}y^{-2}$: but also $[gy, x] = [y, x] = y^{-2}$, so $g^2 = 1$, a contradiction. Thus we have shown that C has no elements of order 4.

Now by what we have already proved the elements in C with odd order commute with each other and form an abelian subgroup O. The elements of C with order a power of 2 form an elementary abelian 2-group E_1 and $C = E_1 \times O$. Hence $G = CQ = (QE_1) \times O$. Since E_1 is elementary abelian, we can write $E_1 = (Q \cap E_1) \times E$ for some subgroup E. Thus $G = (QE) \times O = Q \times E \times O$.

The converse is much easier. Assume that G has the prescribed form $Q \times E \times O$ and let $H \leq G$. Then by Exercise 5.2.12 we have

$$H = (H \cap (Q \times E)) \times (H \cap O)$$

and clearly $H \cap O \lhd G$; thus we can assume that $G = Q \times E$. If $H \cap Q = 1$, then H lies in the subgroup of all elements g of G such that $g^2 = 1$: this subgroup lies in ζG, so $H \lhd G$. Finally if $H \cap Q \neq 1$, then $H \geq Q' = G'$ and again $H \lhd G$. □

Extra-Special p-Groups

A finite p-group G is called *extra-special* if G' and ζG coincide and have order p. These groups play an important role in some of the deeper parts of finite group theory. As examples one thinks of Q_8 and D_8: indeed any non-abelian group of order p^3 is extra-special (Exercise 5.3.6).

Let G be an extra-special p-group and write $C = \zeta G = G'$. This has order p, so it is cyclic: let c be a fixed generator. If $x, g \in G$, then $[x, g^p] = [x, g]^p = 1$ and $g^p \in C$. Consequently $V = G/C$ is an elementary abelian p-group and may be regarded as a vector space over GF(p). If $x, y \in G$, the commutator $[x, y]$ depends only on the cosets $u = xC$ and $v = yC$, so that it is meaningful to write $[x, y] = c^{f(u,v)}$. Thus $f\colon V \times V \to GF(p)$ is a well-defined function. Now $[xx_1, y] = [x, y][x_1, y]$ and $[x, y] = [y, x]^{-1}$, from which it follows that f is a skew-symmetric bilinear form on V. If $f(u, v) = 0$ for all v in V, then $[x, y] = 1$ for all y in G; in this event $u = xC = 0_V$. Thus f is a *nondegenerate* form.

We shall now quote a standard theorem in linear algebra on nondegenerate skew-symmetric bilinear forms. There exists a direct sum decomposition $V = V_1 \oplus \cdots \oplus V_n$ where V_i is a 2-dimensional subspace with basis $\{u_i, v_i\}$ such that $f(u_i, v_i) = 1$, $f(u_i, v_j) = 0$ if $i \neq j$, and $f(u_i, u_j) = 0 = f(v_i, v_j)$ for all i, j.

Write $u_i = x_iC$ and $v_i = y_iC$. Then $G_i = \langle x_i, y_i \rangle$ is a nonabelian group of order p^3. Clearly $C < G_i \leq G$ and $G = G_1G_2 \cdots G_n$. In addition $G/C = \text{Dr}_i\, G_i/C$ and $[G_i, G_j] = 1$ if $i \neq j$. The order of G is, of course, p^{2n+1}.

Central Products

It is natural to think of the extra-special p-group G as a direct product of the groups G_i in which the centers of the G_i are identified. Of course G_i has order p^3, and there are in fact just two possible isomorphism types for G_i (Exercise 5.3.6).

More generally a group G is said to be the *central product* of its normal subgroups $G_1, \ldots, G_n$ if $G = G_1G_2 \cdots G_n$, $[G_i, G_j] = 1$ for $i \neq j$, and $G_i \cap \prod_{j \neq i} G_j = \zeta G$ for all i. Since $\zeta G_i \leq \zeta G$, it follows that $\zeta G_i = \zeta G$. We can sum up our conclusions about extra-special p-groups in terms of central products.

5.3.8. *An extra-special p-group is a central product of n nonabelian subgroups of order p^3 and has order p^{2n+1}. Conversely a finite central product of nonabelian groups of order p^3 is an extra-special p-group.*

For a more precise statement see Exercise 5.3.7.

EXERCISES 5.3

1. Prove that Hamilton's quaternions are realized by the *Pauli spin matrices*

$$i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

by showing that these generate a subgroup of $GL(2, \mathbb{C})$ isomorphic with Q_8.

2. A group of order p^n is isomorphic with a subgroup of the standard wreath product $\mathbb{Z}_p \wr \cdots \wr \mathbb{Z}_p$ (n factors).

3. Find the upper and lower central series of Q_{2^n}.

4. Prove that $\operatorname{Aut} Q_{2^n} \simeq \operatorname{Hol}(\mathbb{Z}_{2^{n-1}})$ if $n > 3$, but that $\operatorname{Aut} Q_8 \simeq S_4$.

*5. If $G = \langle x, y \mid x^2 = 1 = y^{2^n}, y^x = y^{1+2^{n-1}} \rangle$, prove that Aut G is a 2-group.

6. Let G be a nonabelian group of order p^3. If p is odd, prove that G is isomorphic with

$$\langle x, y \mid x^p = 1 = y^p, [x, y]^x = [x, y] = [x, y]^y \rangle$$

or

$$\langle x, y \mid x^{p^2} = 1 = y^p, x^y = x^{1+p} \rangle.$$

Show that these groups have exponent p and p^2 respectively. If $p = 2$, prove that that $G \simeq D_8$ or Q_8. Note that G is always extra-special.

7. Let G be an extra-special group of order p^{2n+1}.
   (i) If $p = 2$, prove that G is a central product of D_8's or a central product of D_8's and a single Q_8. [*Hint*: Show that a central product of two Q_8's is a central product of two D_8's.]
   (ii) If $p > 2$, prove that either G has exponent p or else it is a central product of nonabelian groups of order p^3 and exponent p and a single nonabelian group of order p^3 and exponent p^2.
   (iii) Deduce that there exist two isomorphism types of extra-special groups of order p^{2n+1} and give a presentation of each type.

8. A finite p-group G will be called *generalized extra-special* if ζG is cyclic and G' has order p.
   (i) Prove that $G' \leq \zeta G$ and $G/\zeta G$ is an elementary abelian p-group of even rank.
   (ii) Express G as a central product of groups of two types.
   (iii) Prove that there are two isomorphism types of generalized extra-special groups once the order and index of the centre are specified. Give presentations for these types.

9. Let G be a finite p-group. Prove that G is not abelian but every proper quotient group of G is abelian if and only if G is a generalized extra-special group.

10. Let G be a group of order p^n. If G has a unique subgroup of order p^m for all $1 < m < n$, prove that G is cyclic.

11. If in a finite p-group every subgroup of order p^2 is cyclic, the group is cyclic or generalized quaternion.

5.4. Soluble Groups

Let us begin by expanding our list of examples of finite soluble groups.

5.4.1. *If p, q, r are primes, all groups of orders p^m, p^mq, p^2q^2, or pqr are soluble.*

Proof. Of course a group of order p^m is nilpotent and hence soluble. Let $|G| = p^mq$ and suppose that $|G|$ is minimal subject to G being insoluble: thus $p \neq q$. If N is a proper nontrivial normal subgroup, both N and G/N are soluble by minimality of $|G|$: this implies that G is soluble. It follows that G must be a simple group.

Let n_p be the number of Sylow p-subgroups of G. Then n_p divides q, so that $n_p = q$: for if n_p were 1, there would be a normal Sylow p-subgroup. Let $I = P_1 \cap P_2$ be an intersection of two distinct Sylow p-groups which has maximal order. If $I = 1$, every pair of distinct Sylow p-subgroups intersects trivially, whence the number of nontrivial p-elements in G is $q(p^m - 1) = p^mq - q$. The other elements are q in number, so they must form a unique Sylow q-subgroup, contradicting the simplicity of G. Hence $I \neq 1$.

Now 5.2.4 shows that $I < N_i = N_{P_i}(I)$, and clearly $I \lhd J = \langle N_1, N_2 \rangle$. If J is a p-group, it is contained in some Sylow p-subgroup, say P_3, and $P_1 \cap P_3 \geq P_1 \cap J \geq N_1 > I$, which contradicts the maximality of I. Thus J is not a p-group and q divides $|J|$. If Q is a Sylow q-subgroup of J, then $|QP_1| = p^mq$ and $G = QP_1$, from which we deduce that $I^G = I^{P_1} \leq P_1$, so that I^G is a proper normal subgroup of G, a final contradiction.

Suppose G is an insoluble group of order p^2q^2: by the first part we may assume G simple and $p > q$. Now $n_p \equiv 1 \bmod p$ and $n_p | q^2$, whence $n_p = q^2$. Suppose that P_1 and P_2 are two distinct Sylow p-subgroups such that $I = P_1 \cap P_2 \neq 1$. We note that P_i is abelian since $|P_i| = p^2$, so that $I \lhd P_i$ and therefore $I \lhd \langle P_1, P_2 \rangle = J$. Hence $J \neq G$, from which we infer that $|G:J| = q$. But 1.6.9 implies that $|G|$ divides $q!$, which is impossible since $p > q$. Hence all pairs of distinct Sylow p-subgroups of G intersect trivially. Just as in the preceding case this leads to a unique Sylow q-subgroup.

The final part is left as an exercise for the reader. □

More generally there is a famous theorem of Burnside to the effect that *a group of order p^mq^n is always soluble*: this is proved in Chapter 8. An even

more remarkable theorem due to Feit and Thompson [a46] asserts that *every group of odd order is soluble*; the proof is exeedingly difficult.

The first example of an insoluble group is the alternating group A_5, which has order $60 = 2^2 \cdot 3 \cdot 5$ (Exercise 5.4.2). Thus groups of order p^2qr need not be soluble and 5.4.1 cannot be extended in this direction.

Composition Factors, Principal Factors, and Maximal Subgroups

If G is a group—possibly without a composition series—we shall extend our previous usage and say that H/K is a *composition factor* of G if H is subnormal in G and H/K is simple. Similarly we shall say that H/K is a *principal factor* if H/K is a minimal normal subgroup of G/K.

The following easy lemma exhibits a relation between maximal subgroups and principal factors.

5.4.2. *Let G be a group. Assume that $G = HA$ where H is a proper subgroup and A is an abelian normal subgroup of G. Then H is maximal in G if and only if $A/H \cap A$ is a principal factor of G. Also $|G : H| = |A : H \cap A|$.*

Proof. Note first of all that $H \cap A \lhd H$ and also that $H \cap A \lhd A$ since A is abelian; thus $H \cap A \lhd HA = G$.

Assume that H is maximal. If $H \cap A < L \leq A$ and $L \lhd G$, then $G = HL$ because $L \nleq H$. Hence $A = (HL) \cap A = (H \cap A)L = L$ by the modular law. Hence $A/H \cap A$ is a principal factor. Conversely suppose that $A/H \cap A$ is a principal factor. Let $H < K \leq G$. Then $K = K \cap (HA) = H(K \cap A) > H$. Hence $H \cap A < K \cap A \lhd G$, so that $A = K \cap A$ and $G = K$, which shows that H is maximal. □

5.4.3. *Let G be a soluble group.*

(i) *A composition factor of G has prime order.*
(ii) *A principal factor of G is either an elementary abelian p-group or else a direct product of copies of the additive group of rational numbers.*
(iii) *The index of a maximal subgroup of G is either infinite or a power of a prime.*

Proof. (i) is clear.

(ii) It is enough to prove the result for H a minimal normal subgroup of G. Now $H' \lhd G$ and $H' \neq H$ because H is soluble. Hence $H' = 1$ and H is abelian. If p is a prime, then $H[p] = \{x \in H | x^p = 1\}$ is a normal subgroup of G contained in H. Hence either $H[p] = H$, so that H is an elementary abelian p-group, or $H[p] = 1$ for all p, which means that H is torsion-free.

In the last case one also has $H^p \lhd G$; thus $H^p = H$ and H is a divisible abelian group. The result now follows from 4.1.5.

(iii) Let M be maximal in G. Since G is soluble and $M \neq G$, there is a largest integer i such that $A = G^{(i)} \nleq M$. Then $A' \leq M$ and M/A' is maximal in G/A'. Without loss of generality we can assume that $A' = 1$ and A is abelian. Since M is maximal, $G = MA$. Then 5.4.2 shows that A is minimal normal in G. Since $|G:M| = |A|$, the result follows from (ii). □

The Fitting Subgroup of a Soluble Group

The Fitting subgroup of a soluble group plays a role similar to that of the center of a nilpotent group; the following result may be compared to 5.2.1 and 5.2.3.

5.4.4. *Let G be a soluble group with Fitting subgroup F.*

(i) *If $1 \neq N \lhd G$, then N contains a nontrivial normal abelian subgroup of G and $N \cap F \neq 1$.*
(ii) $C_G(F) = \zeta F$.

Proof. (i) Let i be the largest integer such that $N \cap G^{(i)} \neq 1$; then $(N \cap G^{(i)})' \leq N \cap G^{(i+1)} = 1$, so that $N \cap G^{(i)}$ is abelian and normal in G.

(ii) Suppose that $C = C_G(F)$ is not contained in F. By (i) there exists $A/F \lhd G/F$ such that $F < A \leq CF$ and A/F is abelian. But $A = A \cap (CF) = (A \cap C)F$ and $\gamma_3(A \cap C) \leq [A', C] \leq [F, C] = 1$, which shows that $A \cap C \leq F$ and $A = F$. By this contradiction $C \leq F$ and hence $C = \zeta F$. □

The Nilpotent Length

If G is a finite group, the *upper nilpotent series* $1 = U_0(G) \leq U_1(G) \leq \cdots$ is defined by $U_{i+1}(G)/U_i(G) = \text{Fit}(G/U_i(G))$. The *lower nilpotent series* $G = L_0(G) \geq L_1(G) \geq L_2(G) \geq \cdots$ is defined dually by writing $L_{i+1}(G) = \bigcap_{j=1,2,\ldots} \gamma_j(L_i(G))$, so that $L_i(G)/L_{i+1}(G)$ is the largest nilpotent quotient group of $L_i(G)$. The terms of these series are characteristic—even fully-invariant in the case of $\{L_i(G)\}$—and the factors are nilpotent.

5.4.5. *Let $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ be a series with nilpotent factors in a finite soluble group G. Then*

$$G_i \leq U_i(G) \quad \textit{and} \quad L_i(G) \leq G_{n-i}.$$

In particular

$$U_n(G) = G \quad \textit{and} \quad L_n(G) = 1.$$

The proof is by induction on i. Note that $G_1 \leq G_1^G \leq U_1$ by 5.2.8. It follows immediately that the lengths of the upper and lower nilpotent series of a finite soluble group are equal: this number is called the *nilpotent length.*

It is sometimes convenient to speak of the nilpotent length of an *infinite* soluble group. This is best defined as the length of a shortest series with nilpotent factors. Groups with nilpotent length at most 2 are called *metanilpotent groups.*

Supersoluble Groups

A group is said to be *supersoluble* (or *supersolvable*) if it has a *normal cyclic series*, that is, a series of normal subgroups whose factors are cyclic. Supersoluble groups are, of course, soluble. The group A_4, which has no normal cyclic subgroups except 1, is the first example of a soluble group that is not supersoluble. It is easy to prove—and the reader should check—that *the class of supersoluble groups is closed with respect to forming subgroups, images, and finite direct products.*

5.4.6.

(i) *Supersoluble groups satisfy the maximal condition.*
(ii) *Finitely generated nilpotent groups are supersoluble.*

Proof. This follows from 3.1.7 and 5.2.18. □

5.4.7. *A principal factor of a supersoluble group has prime order and a maximal subgroup has prime index.*

Proof. Let N be a minimal normal subgroup of a supersoluble group G and let $1 = G_0 < G_1 < \cdots < G_n = G$ be a normal cyclic series. Now there is a least integer i that $N \cap G_i \neq 1$. Then $N \cap G_i \lhd G$, so that $N \cap G_i = N$ and $N \leq G_i$. Since $N \cap G_{i-1} = 1$, we obtain $N \simeq NG_{i-1}/G_{i-1} \leq G_i/G_{i-1}$. Hence N is cyclic of prime order. The second statement may be proved just like 5.4.3 (iii). □

In fact the properties of 5.4.7 characterize finite supersoluble groups. This is obvious for the first property; for the second it will be proved in Chapter 9.

5.4.8 (Zappa). *If G is a supersoluble group, there is a normal series*

$$1 = G_0 < G_1 < \cdots < G_n = G$$

in which each factor is cyclic of prime or infinite order and the order of the factors from the left is this: odd factors in descending order of magnitude, infinite factors, factors of order 2.

Proof. By refining a normal cyclic series of G we obtain a normal cyclic series $1 = H_0 < H_1 < \cdots < H_m = G$ in which each factor has prime or infinite order. We describe a procedure for obtaining a new series in which the factors have the stated ordering.

Suppose that H_{i+1}/H_i has order p and H_i/H_{i-1} has order q where $q < p$. Since $|\mathrm{Aut}(H_i/H_{i-1})| = q - 1$, which is not divisible by p, the factor H_i/H_{i-1} lies in the center of H_{i+1}/H_{i-1} and the latter is cyclic of order pq. If $\bar{H}_i/H_{i-1}$ is the subgroup of order p, it is characteristic in H_{i+1}/H_{i-1} and $\bar{H}_i \lhd G$: also $H_{i+1}/\bar{H}_i$ has order q. Replacing H_i by $\bar{H}_i$ we obtain a normal cyclic series of G in which the p-factor now *precedes* the q-factor.

Next let H_{i+1}/H_i have odd prime order p and let H_i/H_{i-1} be infinite cyclic. Then $\mathrm{Aut}(H_i/H_{i-1})$ has order 2, which shows that H_i/H_{i-1} lies in the center of H_{i+1}/H_{i-1} and the latter is abelian. If H_{i+1}/H_{i-1} is infinite cyclic, simply delete H_i from the series. Otherwise there is a subgroup $\bar{H}_i/H_{i-1}$ of order p; then $\bar{H}_i \lhd G$ and $H_{i+1}/\bar{H}_i$ is infinite cyclic. Replacing H_i by $\bar{H}_i$, we cause the p-factor to *precede* the infinite factor.

Finally suppose that H_{i+1}/H_i is infinite and H_i/H_{i-1} has order 2. Then $H_{i+1}/H_{i-1} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}$ and $\bar{H}_i/H_{i-1} = (H_{i+1}/H_{i-1})^2$ is infinite cyclic. Also $\bar{H}_i \lhd G$ and $|H_{i+1} : \bar{H}_i| = 4$. By 5.4.7 there exists $\bar{\bar{H}}_i \lhd G$ such that $\bar{H}_i < \bar{\bar{H}}_i < H_{i+1}$ and $|H_{i+1} : \bar{\bar{H}}_i| = 2 = |\bar{\bar{H}}_i : \bar{H}_i|$. Delete H_i and insert $\bar{H}_i$ and $\bar{\bar{H}}_i$. Thus, at the expense of adding a factor of order 2 on the right, we may move an infinite factor to the left past one of order 2.

By repeated use of these techniques a series of the type sought is obtained. □

5.4.9. *The elements of odd order in a supersoluble group form a characteristic subgroup.*

This follows directly from 5.4.8. Notice however that since the infinite dihedral group is generated by elements of order 2, the elements of finite order in a supersoluble group do not in general form a subgroup.

Finally, we prove a result showing that the Fitting subgroup of a supersoluble group is relatively large.

5.4.10. *If G is a supersoluble group, then* Fit G *is nilpotent and $G/$*Fit G *is a finite abelian group. In particular, G' is nilpotent.*

Proof. Let $F = \mathrm{Fit}\, G$. By 5.4.6 the group G satisfies the maximal condition and F is finitely generated. Hence F is a product of *finitely many* nilpotent normal subgroups and so it is nilpotent by Fitting's theorem (5.2.8). Let $1 = G_0 < G_1 < \cdots < G_n = G$ be a normal cyclic series. Set $F_i = G_{i+1}/G_i$ and $C = \bigcap_{i=1,\ldots,n} C_G(F_i)$. Now Aut F_i is finite and abelian, which shows that G/C is finite and abelian. Also $[G_{i+1} \cap C, C] \leq G_i \cap C$, whence the $G_i \cap C$ form a central series of C and C is nilpotent. Hence $C \leq F$ and G/F is finite and abelian. □

A discussion of the deeper properties of finite soluble groups is deferred until Chapter 9. In the remainder of this chapter we shall be concerned with certain important classes of infinite soluble groups.

Infinite Soluble Groups

We begin with a simple but frequently used fact.

5.4.11. *A finitely generated soluble torsion group is finite.*

Proof. Let G be the group in question and let d denote its derived length. If $d = 0$, there is nothing to prove. So let $d > 0$ and put $A = G^{(d-1)}$. Then by induction on d the quotient group G/A is finite, which by 1.6.11 implies that A is finitely generated. We now use 4.2.9 to show that A is finite, from which it follows that G is finite. □

Polycyclic Groups

One of the most important classes of infinite soluble groups is the class of polycyclic groups. Recall that a group G is said to be *polycyclic* if it has a *cyclic series*, by which we mean of course a series with cyclic factors. It is clear that polycyclic groups are soluble and that every supersoluble group is polycyclic. Moreover the class of polycyclic groups is closed with respect to forming subgroups, images, and extensions. Most of the results that follow are due to K.A. Hirsch who initiated the study of polycyclic groups in 1938.

5.4.12. *A group is polycyclic if and only if it is soluble and satisfies the maximal condition.*

Proof. Every cyclic group satisfies the maximal condition and the latter property is closed under forming extensions (3.1.7); hence every polycyclic group has max. Conversely, suppose that G is a soluble group with max. Then the factors of the derived series are finitely generated abelian groups. By refining this series we obtain one with cyclic factors, thus showing that G is polycyclic. □

5.4.13. *In a polycyclic group G the number of infinite factors in a cyclic series is independent of the series and hence is an invariant of G (known as the* Hirsch length*).*

Proof. Suppose that we have a cyclic series of G: then a refinement of this series is also cyclic and it will have the same number of *infinite* factors. The reason is that if H/K is an infinite cyclic factor and $K \leq K^* < H^* \leq H$,

then *one* of K^*/K, H^*/K^*, and H/H^* is infinite cyclic while the others are finite. Since any two cyclic series have isomorphic refinements, they must have the same number of infinite cyclic factors. □

5.4.14. *A group is polycyclic if and only if it has a normal series each factor of which is either free abelian of finite rank or finite elementary abelian.*

We leave the easy proof as an exercise.

Poly-Infinite Cyclic Groups

Extending our use of the prefix "poly," let us call a group *poly-infinite cyclic* if it has a series with infinite cyclic factors. Obviously every poly-infinite cyclic group is torsion-free and polycyclic, but the converse is false (see Exercise 5.4.15). Nevertheless general polycyclic groups are quite close to being poly-infinite cyclic, as the following theorem shows.

5.4.15.

(i) *Every polycyclic group has a normal poly-infinite cyclic subgroup of finite index.*
(ii) *An infinite polycyclic group contains a nontrivial torsion-free abelian normal subgroup.*

Proof. (i) Let $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ be a cyclic series in a polycyclic group G. If $n \leq 1$, then G is cyclic and the result is obvious. Let $n > 1$ and put $N = G_{n-1}$. By induction on n there is a normal subgroup M of N such that M is poly-infinite cyclic and N/M is finite. Now N/M_G is finite because it is a finitely generated torsion group (see 5.4.11), and M_G is poly-infinite cyclic. Thus nothing is lost if we assume that $M \lhd G$. If G/N is finite, so is G/M and we are finished. Assume therefore that G/N is infinite cyclic, generated by xN say.

There is a positive integer r for which x^r centralizes N/M. Set $L = \langle x^r, M \rangle$. Then it is clear that $L \lhd \langle x, N \rangle = G$. Moreover G/L is finite because it is the product of the finite subgroups $\langle x, L \rangle/L$ and NL/L. Since no positive power of x can belong to N, the factor L/M is infinite cyclic and L is poly-infinite cyclic.

(ii) If G is infinite, then $L \neq 1$ and the smallest nontrivial term of the derived series of L is a subgroup of the type sought. □

We shall establish next an interesting property of subgroups of polycyclic groups.

5.4.16 (Mal'cev). *Let H be a subgroup of a polycyclic group G. Then H equals the intersection of all the subgroups of finite index in G that contain H.*

Proof (J.S. Wilson). We begin with the remark that all is well if G is abelian. For then $H \lhd G$ and G/H, being a finitely generated abelian group, is residually finite by Exercise 4.2.15; this gives the desired result.

In the general case let l be the Hirsch length of G. Should $l = 0$, the group will be finite and there is nothing to prove. Assume therefore that $l > 0$ and proceed by induction on l. According to 5.4.15 there is a torsion-free abelian normal subgroup $A \neq 1$. Since the Hirsch length of G/A is less than l, the theorem is true for G/A.

Let $g \in G \backslash H$; it suffices to find a subgroup K such that $H \leq K$, $|G:K| < \infty$ and $g \notin K$. If $g \notin HA$, the existence of such a K may be inferred from the truth of the theorem for G/A. Assume therefore that $g \in HA$. Then $g = ha$ where $h \in H$ and $a \in A$; notice that $a \notin H \cap A$ since $g \notin H$.

By the abelian case there is a subgroup B of A such that $H \cap A \leq B$, $|A:B| < \infty$ and $a \notin B$. Clearly $A^m \leq B$ for some $m > 0$, and $|A:A^m| < \infty$. By induction on l the theorem is true for G/A^m, so we can assume that $g \in HA^m$, say $g = h_1 a_1$, where $h_1 \in H$ and $a_1 \in A^m$. Hence $ha = h_1 a_1$, so that $aa_1^{-1} = h^{-1}h_1 \in H \cap A \leq B$. Since $a_1 \in A^m \leq B$, we reach the contradiction $a \in B$. □

Specializing to the case $H = 1$ we obtain

5.4.17 (Hirsch). *A polycyclic group is residually finite.*

An arbitrary group G can be made into a topological group by declaring the collection of all subgroups of finite index to be a base of neighborhoods of the identity. The resulting topology is known as the *profinite topology*: it is Hausdorff precisely when G is residually finite. Mal'cev's theorem may be reformulated by saying that *every subgroup of a polycyclic group is closed in the profinite topology.*

We give next a further application of 5.4.15.

5.4.18 (Hirsch). *If a polycyclic group G is not nilpotent, then it must have a finite nonnilpotent image.*

Proof. Let G be a counterexample with minimal Hirsch length. Certainly G will be infinite, so 5.4.15 provides us with a nontrivial torsion-free abelian normal subgroup A. Of course A is free abelian; let r be its rank.

If p is any prime, G/A^p has smaller Hirsch length than G, so by minimality G/A^p is nilpotent. Now A/A^p is elementary abelian of order p^r; thus by 5.2.1 it lies in $\zeta_r(G/A^p)$ and

$$B = [A, \underbrace{G, \ldots, G}_{r}] \leq A^p.$$

But $\bigcap_p A^p = 1$ because A is free abelian. Hence $B = 1$ and $A \leq \zeta_r G$. This shows that G is nilpotent, a contradiction. □

This result is very useful in transferring properties of finite groups to polycyclic groups. Here are some examples due to Hirsch and Itô.

5.4.19. *The Frattini subgroup of a polycyclic group is nilpotent.*

Proof. Let $F = \text{Frat } G$ where G is polycyclic. If F is not nilpotent, then some finite F/N is not nilpotent. Replacing N by its core in G, we can suppose that $N \lhd G$. But $\text{Frat}(G/N) = F/N$ and a finite Frattini subgroup is always nilpotent by 5.2.15 (i). This is a contradiction. □

5.4.20. *If G is a polycyclic and $G' \leq \text{Frat } G$, then G is nilpotent.*

Proof. If G is not nilpotent, it has a finite nonnilpotent image H. But $H' \leq \text{Frat } H$ is clearly valid and by 5.2.16 this implies that H is nilpotent. □

For a detailed study of polycyclic groups the reader should consult the book by Segal [b61].

Finitely Generated Soluble Groups

These form a much wider class of groups than do polycyclic groups. An example of a finitely generated soluble group that is not polycyclic is the semidirect product

$$G = X \ltimes A$$

where A is the additive group of dyadic rationals $m2^n$, $m, n \in \mathbb{Z}$, and $X = \langle x \rangle$ is an infinite cyclic group acting on A via multiplication by 2: thus $ax = 2a$. This group is generated by x and the integer 1: also it is metabelian. However G is not polycyclic because A is not finitely generated.

Soluble groups with the *maximal condition on normal subgroups*, max-*n*, are intermediate between polycyclic groups and finitely generated soluble groups, as we now show.

5.4.21. *A soluble group G with the maximal condition on normal subgroups is finitely generated.*

Proof. Let d denote the derived length of G. If $d \leq 1$, then G is abelian and the assertion is obvious. Let $d > 1$ and put $A = G^{(d-1)}$. By induction on d there is a finite set of generators $x_1 A, \ldots, x_m A$ for G/A. Now A satifies max-G since G satisfies max-n. Hence $A = a_1^G \cdots a_n^G$ for some finite set of elements a_i. But since A is abelian, $a_i^G = a_i^{\langle x_1, \ldots, x_m \rangle}$. Therefore G is generated by $a_1, \ldots, a_n, x_1, \ldots, x_m$. □

Much more will be said of finitely generated soluble groups in Chapter 15.

Soluble Groups with the Minimal Condition

Since polycyclic groups have been identified as the soluble groups with max, it is natural to ask about the dual class, soluble groups with min. If G is a soluble group with min, each factor of an abelian series has min and so by 4.2.11 is a direct product of finitely many cyclic and quasicyclic groups. Thus *the soluble groups with min are exactly the poly-(finite cyclic or quasicyclic) groups.*

Basic in the study of the minimal condition is

5.4.22. *Let the group G satisfy the minimal condition on normal subgroups. Then G possesses a unique minimal subgroup of finite index (called the* finite residual). *This subgroup is characteristic in G.*

Proof. The minimal condition on normal subgroups guarantees the existence of a smallest *normal* subgroup of finite index, say F. Let H be any subgroup of finite index. By 1.6.9 the core H_G has finite index, so by 1.3.12 we have $|G: H_G \cap F| < \infty$. Hence $H_G \cap F = F$ and $F \leq H$, showing that F is contained in every subgroup with finite index in G. □

We come now to the structure theorem for soluble groups with min.

5.4.23 (Černikov). *A soluble group satisfies the minimal condition if and only if it is an extension of a direct product of finitely many quasicyclic groups by a finite group.*

Proof. Let G be a soluble group with min and let F be its finite residual (see 5.4.22). Then we can assume that $F \neq 1$ since G/F is finite. Therefore F contains a nontrivial normal abelian subgroup of G, say A, by 5.4.4. Let $1 \neq a \in A$. Clearly conjugates of a have the same order as a and belong to A. Now according to Exercise 4.3.5 in an abelian group with min there are only finitely many elements of each prescribed order. Hence $|G: C_G(a)| < \infty$. By definition of F we have $F \leq C_G(a)$ and consequently $a \in \zeta F$ and $\zeta F \neq 1$.

If $F = \zeta F$, then F is abelian with min and has no proper subgroups of finite index: therefore F is a direct product of finitely many quasicyclic groups by 4.2.11, and G has the required structure. Thus we can assume that $\zeta F < F$. Now $\zeta F \lhd G$, so the preceding argument may be applied to the group $G/\zeta F$ (which has finite residual $F/\zeta F$) to show that $\zeta F = \zeta_1 F < \zeta_2 F$. Let $z \in \zeta_2 F \backslash \zeta_1 F$ and let $x \in F$; then $z^x = zz_1$ where $z_1 \in \zeta_1 F$. Now the minimal condition implies that G is a torsion group; hence $|z_1|$ divides $|z|$. Since ζF has min, for a given z there are only finitely many possibilities for z_1 in $\zeta_1 F$ and hence for z^x where $x \in F$. Thus $|F: C_F(z)| < \infty$, which implies that $F = C_F(z)$ and $z \in \zeta_1 F$, a contradiction.

The converse follows from the fact that a quasicyclic group satisfies min and min is closed under extensions (3.1.7). □

A group which is an extension of a finite direct product of quasicyclic groups by a finite group is called a *Černikov group*. Such groups arise rather frequently in infinite group theory. Indeed until very recently they were the only known examples of groups with min. In this connection see 14.4.

Exercises 5.4

1. Let p, q, r be primes. Prove that a group of order pqr is soluble.
2. If G is an insoluble group of order at most 200, prove that $|G| = 60$, 120, 168, or 180.
3. Give examples of insoluble groups of orders 60, 120, 168, and 180.
4. A group is called *perfect* if it equals its derived subgroup.
   (a) Prove that every group G has a unique maximal perfect subgroup R and R is fully-invariant in G.
   (b) If G is finite, then R is the smallest term of the derived series.
   (c) If G is perfect but not simple and $1 < |G| \leq 200$, show that $|G| = 120$ or 180.
   (d) Find a perfect nonsimple group of order 120 (in fact there are no perfect groups of order 180—see Exercise 10.1.5).
5. The class of supersoluble groups is closed with respect to forming subgroups, images, and finite direct products.

*6. The product of two normal supersoluble subgroups need not be supersoluble. [*Hint*: Let X be the subgroup of GL(2, 3) generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

thus $X \simeq D_8$. Let X act in the natural way on $A = \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and write $G = X \ltimes A$. Show that G is not supersoluble. Let L and M be distinct Klein 4-subgroups of X and consider $H = LA$ and $K = MA$.]

7. If N is a normal nilpotent subgroup of G and G/N' is supersoluble, then G is supersoluble.
8. If $R = \mathbb{Z}$ or $\mathbb{Z}_p$, prove that the group of triangular matrices $T(n, R)$ is supersoluble.
9. If N is a normal subgroup of a polycyclic group G, prove that $h(G) = h(N) + h(G/N)$ where $h(X)$ denotes the Hirsch length of X. Deduce that $h(G) = h(G/N)$ if and only if N is finite.
10. If H is a subgroup of a polycyclic group G, prove that $h(G) = h(H)$ if and only if $|G : H|$ is finite.
11. A group is said to be *poly-(cyclic or finite)* if it has a series whose factors are cyclic or finite. Prove that a group is poly-(cyclic or finite) if and only if it has a normal polycyclic subgroup of finite index.
12. Prove that 5.4.15–5.4.20 are valid for poly-(cyclic or finite) groups.

13. (Seksenbaev). If a polycyclic group G is a residually finite p-group for infinitely many primes p, then it is a finitely generated torsion-free nilpotent group (cf. 5.2.21). [*Hint*: Assume that G is not nilpotent. Show that $\gamma_i G/\gamma_{i+1} G$ is finite for some i. Now argue that $|\gamma_i G : \gamma_{i+1} G|$ is divisible by infinitely many primes.]

14. (Šmelkin). Let G be a polycyclic group and p any prime. Then G has a normal subgroup of finite index which is a residually finite p-group. [*Hint*: Argue by induction on the length of a cyclic series.]

15. (Hirsch). Let G be the group with generators x, y, z and defining relations $x^z = x^{-1}$, $y^z = y^{-1}$ and $[x, y] = z^4$. Prove that G is a torsion-free polycyclic group with $h(G) = 3$. Show also that G_{ab} is finite, so that G is not poly-infinite cyclic.

16. If G is a finitely generated nilpotent group, prove that G is isomorphic with a subgroup of the direct product of a finite nilpotent group and a finitely generated torsion-free nilpotent group.

17. A group is poly-(quasicyclic or finite) precisely when it is a Černikov group.

18. (M.F. Newman). Let G be an infinite Černikov p-group. Assume that G is not abelian but every proper quotient group of G is abelian (see Exercise 5.3.9).
    (i) Show that G is nilpotent of class 2.
    (ii) Show that ζG is of type p^∞ and $|G'| = p$.
    (iii) Prove that $G/\zeta G$ is an elementary abelian p-group of order p^{2n} for some positive n.
    (iv) Find a presentation for G.
    (v) Show that G is determined up to isomorphism by p and n.

19. Show that a maximal subgroup of a polycyclic group has finite index.

20. (Kegel). Let G be a polycyclic group and let H be a subgroup of G such that HN is subnormal in G for every $N \lhd G$ with G/N finite. Prove that H is subnormal in G. [*Hint*: Let $A \lhd G$ where A is free abelian with positive rank r. Argue that one can assume $A/H \cap A$ to be torsion-free. If p is a prime, then HA^p is subnormal in G].

21. Let G be a polycyclic group given by a finite presentation with generators $x_1, \dots, x_n$. Show that there is an algorithm which, when words $w, w_1, \dots, w_m$ in the x_i are given, decides whether $w \in \langle w_1, w_2, \dots, w_m \rangle$ in G. (Then the *generalized word problem* is said to be soluble for G.) [*Hint*: Use 5.4.16 and imitate the proof of 2.2.5.]

CHAPTER 6

Free Groups and Free Products

6.1. Further Properties of Free Groups

Among the basic properties of free groups established in Chapter 2 was the fact that every group is isomorphic with a quotient group of a free group, a fundamental result that demonstrates clearly the significance of free groups. Thus the quotient groups of free groups account essentially for all groups. By contrast subgroups of free groups are very restricted; in fact they too are free. This important fact, first proved in 1921 by Nielsen in the case of finitely generated free groups, is the principal result of the first section.

Subgroups of Free Groups

6.1.1 (The Nielsen–Schreier† Theorem). *If W is a subgroup of a free group F, then W is a free group. Moreover, if W has finite index m in F, the rank of W is precisely $nm + 1 - m$ where n is the rank of F (which may be infinite).*

Of the many approaches to this theorem we have chosen one due to A.J. Weir; this is entirely algebraic in nature, the crucial idea being the introduction of certain functions called coset maps. The notation that follows will remain fixed throughout the proof of the Nielsen–Schreier Theorem.

Let F be a free group on a set X; let W be an arbitrary subgroup of F. The right cosets of W in F are to be labeled by means of an index set I containing the symbol 1,

$$\{W_i | i \in I\},$$

† Otto Schreier (1901–1929).

with the convention that $W_1 = W$. We choose a right transversal to W in F, the representative of the coset W_i being written

$$\overline{W_i},$$

with the stipulation that $\overline{W} = 1$.

If $u \in F$, the elements $\overline{W_i}u$ and $\overline{W_i u}$ belong to the same right coset $W_i u$, so that

$$\overline{W_i}u\overline{W_i u}^{-1} \in W.$$

The idea behind the proof is to find a transversal T such that the nontrivial elements $\overline{W_i}u\overline{W_i u}^{-1}$, $u \in T$, $i \in I$, constitute a set of free generators of W.

With this aim in mind we associate with each i in I and x in X a symbol y_{ix}, denoting by

$$\hat{F}$$

the free group on the set of all y_{ix}. The assignment $y_{ix} \mapsto \overline{W_i}x\overline{W_i x}^{-1}$ determines a homomorphism

$$\tau\colon \hat{F} \to W.$$

The first step is to show that τ is surjective.

Coset Maps

To each u in F and i in I we shall associate an element u^{W_i} of $\hat{F}$, referring to the mapping $u \mapsto u^{W_i}$ as a *coset map.* (Note: u^{W_i} does *not* mean a normal closure in this chapter.)

Define

$$1^{W_i} = 1, \qquad x^{W_i} = y_{ix}, \qquad \text{and} \qquad (x^{-1})^{W_i} = (x^{W_i x^{-1}})^{-1},$$

if $x \in X$. Generally, if $u = vy$ in reduced form with $y \in X \cup X^{-1}$, define u^{W_i} by induction on the length of u by means of the equation

$$u^{W_i} = v^{W_i} y^{W_i v}.$$

It is important to know how a coset map affects products and inverses.

6.1.2. *If u and v belong to F, then $(uv)^{W_i} = u^{W_i} v^{W_i u}$ and $(u^{-1})^{W_i} = (u^{W_i u^{-1}})^{-1}$.*

Proof. Consider the product formula. This certainly holds if $v = 1$. Suppose that $v \in X \cup X^{-1}$. If the last symbol of u is not v^{-1}, the formula is true by definition. Otherwise $u = u_1 v^{-1}$ *in reduced form* and $uv = u_1$. Thus $(uv)^{W_i} = u_1^{W_i}$. But $u^{W_i} = (u_1 v^{-1})^{W_i} = u_1^{W_i}(v^{-1})^{W_i u_1}$ and $(v^{-1})^{W_i u_1} = (v^{W_i u_1 v^{-1}})^{-1} = (v^{W_i u})^{-1}$ by definition. Hence $u_1^{W_i} = u^{W_i} v^{W_i u}$ as required.

Assume now that the length of v (as a reduced word in X) exceeds 1. Write $v = v_1 y$ in reduced form with $y \in X \cup X^{-1}$. By induction on the

length of v

$$\begin{aligned}(uv)^{W_i} = ((uv_1)y)^{W_i} &= (uv_1)^{W_i} y^{W_i uv_1} \\ &= u^{W_i}(v_1^{W_i u}) y^{W_i uv_1} \\ &= u^{W_i} v^{W_i u}.\end{aligned}$$

To prove the formula for $(u^{-1})^{W_i}$ apply the product rule to $u^{-1}u$. □

Now let us compute the composite of a coset map with $\tau\colon \hat{F} \to W$.

6.1.3. *If $u \in F$ and $i \in I$, then $(u^{W_i})^\tau = \overline{W_i u}\,\overline{W_i u}^{-1}$.*

Proof. Induct on the length of u; the equation is true by definition if $u = 1$ or $u \in X \cup X^{-1}$. Write $u = u_1 u_2$ where u_1 and u_2 have smaller length than u. Then by the product rule

$$\begin{aligned}(u^{W_i})^\tau = ((u_1u_2)^{W_i})^\tau &= (u_1^{W_i} u_2^{W_i u_1})^\tau \\ &= \overline{W_i}u_1\,\overline{W_i u_1}^{-1}\,\overline{W_i u_1}u_2\,\overline{W_i u_1 u_2}^{-1} \\ &= \overline{W_i}u\overline{W_i u}^{-1},\end{aligned}$$

as required. □

Next we consider the restriction of the coset map $u \mapsto u^W$ to W; call this

$$\psi\colon W \to \hat{F}.$$

Now 6.1.2 shows that $(uv)^W = u^W v^W$ if $u, v \in W$; thus ψ is a homomorphism. Also by 6.1.3 we have $(u^\psi)^\tau = (u^W)^\tau = \overline{W}u\overline{Wu}^{-1} = u$ if $u \in W$; for $\overline{W} = 1 = \overline{Wu}$. Consequently

$$\psi\tau = 1.$$

It follows that ψ is injective and τ is surjective. Therefore τ is a presentation of W in the y_{ix}; we seek now a set of defining relators for τ, that is, a subset whose normal closure in $\hat{F}$ equals Ker τ. Write

$$\chi = \tau\psi,$$

an endomorphism of $\hat{F}$.

6.1.4. *The group W has a presentation $\tau\colon \hat{F} \to W$ with generators y_{ix} and defining relators $y_{ix}^{-1} y_{ix}^{\chi}$, $(i \in I, x \in X)$.*

Proof. Let N be the normal closure in $\hat{F}$ of the set of all $y_{ix}^{-1}y_{ix}^{\chi}$. Notice that $K = \text{Ker}\,\tau$ equals Ker χ because ψ is injective. Since $\psi\tau = 1$, we have $\chi^2 = \tau(\psi\tau)\psi = \chi$, which shows that $(y_{ix}^{-1}y_{ix}^{\chi})^\chi = 1$. Hence $N \leq K$. Conversely, let $k \in K$; then k is expressible in terms of the y_{ix}. Now $y_{ix}^{\chi} \equiv y_{ix} \bmod N$, so $k^\chi \equiv k \bmod N$ because χ is a homomorphism. Hence $k \in N$ and $K = N$. □

We pass now to a more economical set of relators associated with elements of the transversal.

6.1.5. *If u denotes a nontrivial element of the transversal, then the elements u^W form a set of defining relators for the presentation $\tau: \hat{F} \to W$.*

Proof. If u is a transversal element, $(u^W)^\tau = \overline{Wu}\,\overline{Wu}^{-1} = uu^{-1} = 1$ by 6.1.3. Thus $u^W \in K = \text{Ker}\,\tau$. Let N be the normal closure of the set of all u^W; then $N \leq K$. To prove the reverse inclusion it suffices to show that $y_{ix}^\chi \equiv y_{ix} \bmod N$; this is because of 6.1.4. We find, using 6.1.2 and 6.1.3, that

$$y_{ix}^\chi = (y_{ix}^\tau)^W = (\overline{W_i}x\overline{W_ix}^{-1})^W = \overline{W_i}^W x^{W\overline{W_i}}(\overline{W_ix}^{-1})^{W\overline{W_i}x}.$$

Now $W\overline{W_i} = W_i$, while $(\overline{W_ix}^{-1})^{W\overline{W_i}x} = (\overline{W_ix}^W)^{-1}$ by 6.1.2. Hence

$$y_{ix}^\chi = \overline{W_i}^W x^{W_i}(\overline{W_ix}^W)^{-1} \equiv y_{ix} \mod N$$

since $x^{W_i} = y_{ix}$ and all u^W are in N. □

Schreier Transversals

So far we have constructed a presentation of W for each right transversal. The time has come to make a special choice of transversal which will furnish a presentation of W making the structure of that subgroup clear.

A subset S of F is said to have the *Schreier property* if $v \in S$ whenever $vy \in S$; here $y \in X \cup X^{-1}$ and vy is in reduced form. Thus S contains all initial parts of its members. What we require is a transversal to W which has the Schreier property. However it is not obvious that such a transversal exists and this must first be established.

6.1.6. *There exists a right Schreier transversal to W in F.*

Proof. Define the *length of a coset* to be the minimum length of a word in that coset. The only coset of length 0 is W: to this the representative 1 is assigned. Let W_i be a coset of length $l > 0$ and assume that coset representatives have been assigned to all cosets of length less than l in such a way that the Schreier property holds. There is an element u of length l in W_i; write $u = vy$ where $y \in X \cup X^{-1}$ and v has length $l - 1$. Then $\overline{Wv}$ has already been assigned; we define $\overline{W_i}$ to be $\overline{Wv}y$, observing that initial parts of this $\overline{W_i}$ are in the transversal. In this way a Schreier transversal can be constructed. □

The Nielsen–Schreier Theorem can now be proved.

***Proof of* 6.1.1.** Choose a Schreier transversal to W in F. As usual write $K = \text{Ker}\,\tau = \text{Ker}\,\chi$. We know from 6.1.5 that K is the normal closure of the u^W

where u is a nontrivial element of the transversal. Write $u = vx^\varepsilon$ where $x \in X$, $\varepsilon = \pm 1$ and v has shorter length than u. Then $u^W = v^W(x^\varepsilon)^{Wv}$. Now $x^{Wv} = y_{ix}$ where $W_i = Wv$; also $(x^{-1})^{Wv} = y_{jx}^{-1}$ where $W_j = Wvx^{-1}$. Therefore

$$u^W = v^W y_{kx}^\varepsilon \tag{1}$$

for some k. Now v belongs to the transversal by the Schreier property, so v^W as well as u^W is in K. Hence $y_{kx} \in K$. It follows from (1) that each u^W is expressible in terms of certain y_{kx} which themselves belong to K.

We conclude from the last paragraph that K is the normal closure in $\hat{F}$ of certain free generators y_{kx}. It follows that W is a free group (see Exercise 2.1.5).

Now suppose that $|F : W| = m$ is finite. The rank of $\hat{F}$ is nm. If we can show that exactly $m - 1$ of the y_{ix}'s belong to K, it will follow that W has rank equal to $nm - (m - 1) = nm + 1 - m$.

In the first place $y_{ix} \in K$ if and only if $\overline{W_i}x = \overline{W_i x}$. Take any coset W_i other than W. Delete the final symbol of $\overline{W_i}$ (in reduced form) to obtain another transversal element, say $\overline{W_j}$; then $\overline{W_i} = \overline{W_j}x^\varepsilon$ and $W_i = W_j x^\varepsilon$ for some $x \in X$, $\varepsilon = \pm 1$. If $\varepsilon = 1$, then $\overline{W_j}x\overline{W_j x}^{-1} = 1$ and $y_{jx} \in K$. If $\varepsilon = -1$, then $\overline{W_i}x\overline{W_i x}^{-1} = 1$ and $y_{ix} \in K$. Thus each of the $m - 1$ cosets $W_i \neq W$ furnishes a y_{ix} in K; clearly all these y_{ix} are different. Conversely let $y_{ix} \in K$, so that $\overline{W_i}x = \overline{W_i x}$: let $W_j = W_i x$. The either $W_i \neq W$ or $W_j \neq W$; hence y_{ix} arises from either W_i or W_j. Thus all the y_{ix} in K are obtained in this manner: they are exactly $m - 1$ in number. □

As an illustration of the procedure for finding a set of free generators for a subgroup let us consider the case of the derived subgroup.

6.1.7. *If F is a noncyclic free group, then F' is a free group of infinite rank.*

Proof. Let F be free on the set $\{x_\alpha | \alpha < \beta\}$ where α, β are ordinals. By 2.3.8 the group F/F' is a free abelian group with the set $\{x_\alpha F' | \alpha < \beta\}$ as a basis. Thus each element of F can be written uniquely in the form $cx_{\alpha_1}^{l_1}x_{\alpha_2}^{l_2}\cdots x_{\alpha_k}^{l_k}$ where $\alpha_i < \alpha_{i+1}$, $c \in F'$ and l_i is a nonzero integer. The elements $x_{\alpha_1}^{l_1}x_{\alpha_2}^{l_2}\cdots x_{\alpha_k}^{l_k}$ can be used to form a transversal to F' since no two lie in the same coset. Clearly this is a Schreier transversal. The Schreier method yields a set of free generators of F'. If $\alpha_1 < \alpha_2$, the free generators include

$$\overline{F'x_{\alpha_2}}x_{\alpha_1}(\overline{F'x_{\alpha_2}x_{\alpha_1}})^{-1} = x_{\alpha_2}x_{\alpha_1}(x_{\alpha_1}x_{\alpha_2})^{-1} = x_{\alpha_2}x_{\alpha_1}x_{\alpha_2}^{-1}x_{\alpha_1}^{-1}$$

and these are all different. Hence F' has infinite rank. □

The Reidemeister–Schreier Theorem

The Nielsen–Schreier method has many applications. One of these is a method of writing down a presentation of a subgroup when a presentation of the group is known.

6.1.8 (Reidemeister–Schreier). *Let G be a group and H a subgroup of G. Suppose that $\varphi: F \to G$ is a presentation of G with generators X and relators S. Let W be the preimage of H under φ. Then with the above notation*:

(i) *$\tau\varphi: \hat{F} \to H$ is a presentation of H with generators y_{ix} and defining relators s^{W_i}, u^W where $i \in I$, $s \in S$, and u is a nontrivial element of a transversal to W in F.*
(ii) *If $|G:H| = m$ is finite and G is an n-generator group, then H can be generated by $nm + 1 - m$ elements.*

Proof. (i) Clearly Ker $\tau\varphi$ equals the preimage of Ker $\varphi = K$ under τ. Denote by N the normal closure in $\hat{F}$ of all the s^{W_i} and u^W. Let $s \in S$. Since $S \subseteq K \leq W$, we have $W_i s = W_i$ for all i. Hence $(s^{W_i})^\tau = \overline{W}_i s \overline{W}_i^{-1}$. In addition $(u^W)^\tau = 1$ by 6.1.5; thus N^τ is the normal closure in W of all $\overline{W}_i s \overline{W}_i^{-1}$, which implies that $N^\tau = S^F = \text{Ker } \varphi = K$. Hence Ker $\tau\varphi = N(\text{Ker } \tau) = N$.

(ii) This follows from 6.1.1 since $|F : W| = |G : H| = m$. □

Residual Finiteness of Free Groups

Since every finite group is an image of a free group, free groups must have "many" finite quotient groups. This is true in the following very strong sense.

6.1.9 (Iwasawa). *If p is any prime and F any free group, then F is a residually finite p-group.*

Proof. Let $1 \neq f \in F$. We need to find a homomorphism θ from F to a finite p-group such that $f^\theta \neq 1$. Supposing F to be free on a set X, we may write f in normal form

$$f = x_{i_1}^{m_1} x_{i_2}^{m_2} \cdots x_{i_r}^{m_r}$$

where $x_i \in X$, $m_i \neq 0$, and $i_u \neq i_{u+1}$. Let q be the largest of the positive integers $i_1, i_2, \ldots, i_r$.

Choose a positive integer n such that p^n does not divide $m_1 m_2 \cdots m_r$. Writing E_{uv} for the elementary $(r+1) \times (r+1)$ matrix over $\mathbb{Z}_{p^n}$ with 1 in position (u, v) and 0 elsewhere, we define

$$g_j = \prod_{i_u = j} (1 + E_{uu+1}) \tag{2}$$

for $1 \leq j \leq q$, with the convention $g_j = 1$ should no i_u equal j. Then g_j is an element of the group G of all $(r+1)$-by-$(r+1)$ upper unitriangular matrices over $\mathbb{Z}_{p^n}$. By a remark at the end of 5.1 the group G is a finite p-group.

Since F is free on X, we are at liberty to define a homomorphism $\theta: F \to G$ by means of the rule $x_{i_u}^\theta = g_{i_u}$ if $1 \leq u \leq r$, and $x^\theta = 1$ for all other x in X. Thus $f^\theta = g_{i_1}^{m_1} \cdots g_{i_r}^{m_r}$: we shall show that this element is not 1. Keep in

mind that $E_{uv}E_{vw} = E_{uw}$ while other products of E's vanish. Now the factors of the product (2) commute: for i_u and i_{u+1} cannot both equal j. Expansion of the product gives $g_j^l = 1 + l\sum_{i_u=j} E_{uu+1}$. Multiplying the $g_{i_j}^{m_j}$ together one sees that the term E_{1r+1} occurs in f^θ with coefficient $m_1 m_2 \cdots m_r$, which is not zero in $\mathbb{Z}_{p^n}$. So $f^\theta \neq 1$ and the theorem is proved. □

If F/N is a finite p-group, it is nilpotent, so that $\gamma_i F \leq N$ for some i. Since the intersection of all such N is trivial by 6.1.9, we conclude that the intersection of the $\gamma_i F$ is trivial. This allows us to state an important result.

6.1.10 (Magnus). *If F is a free group, the intersection of all the terms of the lower central series of F is trivial, that is, G is residually nilpotent.*

A noteworthy property of the lower central series of a free group that will not be proved here is that all the factors are free abelian groups. A proof together with a formula for the ranks of the factors may be found in [b31].

Hopficity

A group G is said to be *hopfian* (after H. Hopf†) if it is not isomorphic with a proper quotient group, or, equivalently, if every surjective endomorphism is an automorphism. For example, all finite groups and all simple groups are hopfian, whereas a free abelian group of infinite rank is not.

The original question posed by Hopf in 1932 was: is every finitely generated group hopfian? It is now known that the answer is negative (see Exercise 6.1.16). However there remains the following useful fact.

6.1.11 (Mal'cev). *A finitely generated residually finite group G is hopfian.*

Proof. Suppose that the surjective endomorphism $\theta: G \to G$ is not an isomorphism: let $1 \neq x \in \operatorname{Ker} \theta$. By residual finiteness there is a normal subgroup M of finite index not containing x. Now since G is finitely generated, there are only finitely many ways—let us say n—of mapping G homomorphically to $Q = G/M$. Let $v: G \to G/\operatorname{Ker} \theta$ be the natural homomorphism and $\bar{\theta}$: $G/\operatorname{Ker} \theta \to G$ the isomorphism $g(\operatorname{Ker} \theta) \mapsto g^\theta$. If $\varphi_1, \ldots, \varphi_n$ are the n distinct homomorphisms from G to Q, the $v\bar{\theta}\varphi_i$ are distinct, so they constitute all the homomorphisms from G to Q; in every case x maps to the identity. However in the natural homomorphism $G \to Q$ the element x does not map to the identity. So there are $n + 1$ homomorphisms from G to Q. □

Combining 6.1.9 and 6.1.11 we obtain an interesting result.

† Heinz Hopf (1894–1971).

6.1.12 (Nielsen). *A free group of finite rank is hopfian.*

This has a useful corollary.

6.1.13. *Let F be a free group with finite rank n. If X is a subset of n elements that generates F, then F is free on X.*

Proof. Suppose that F is free on $\{y_1, y_2, \dots, y_n\}$; let $X = \{x_1, x_2, \dots, x_n\}$. The assignments $y_i \mapsto x_i$ determine an endomorphism $\theta: F \to F$ which is clearly surjective. The hopfian property of F shows that θ is an automorphism of F. If some reduced word in the x_i's were trivial, the corresponding reduced word in the y_i's would be trivial, which cannot be true. By 2.1.3 the group F is free on X. □

EXERCISES 6.1

1. If F is a free group and $1 \neq x \in F$, then $C_G(x)$ is cyclic.
2. Prove that a free group satisfies the maximal condition on centralizers of subgroups.
3. Every free group is (directly) indecomposable.
4. Prove that a group which has the projective property is free (see 2.1.6).
5. Show that GL(2, $\mathbb{Z}$) has free subgroups of all countable ranks.
6. Let G be a group which has a presentation with n generators and r relators. If H is a subgroup with finite index m, show that H has a presentation with nm generators and $rm - 1 + m$ relators. Deduce that a subgroup of finite index in a finitely presented group is finitely presented.
7. Let F be a free group of finite rank n. Find the rank of F^2 as a free group.
8. (G. Baumslag). If G is a finitely generated residually finite group, then Aut G is residually finite. Deduce that the automorphism group of a free group of finite rank is residually finite. [*Hint*: Let $1 \neq \alpha \in \text{Aut } G$; then $g^\alpha \neq g$ for some $g \in G$ and $g^{-1}g^\alpha \notin N$ where G/N is finite. Put $M = \bigcap_{\beta \in \text{Aut } G} N^\beta$ and consider $C_{\text{Aut } G}(G/M)$.]
9. A group is said to be *locally free* if every finite subset is contained in a free subgroup. Prove that a group is locally free exactly when its finitely generated subgroups are free.
10. There exist nontrivial locally free groups that are perfect (cf. 6.1.10). [*Hint*: Let F_n be free of rank 2 and consider embeddings $F_n \to F'_{n+1}$.]
11. There exist nontrivial locally free groups that have no proper subgroups of finite index (see 6.1.9).
12. An abelian group of finite Prüfer rank is hopfian if and only if its torsion-subgroup is reduced.

13. A free group which is hopfian must have finite rank.

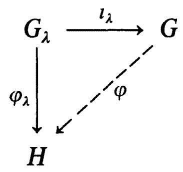
*14. Let F be a free group on a set $\{x_1, \dots, x_n\}$. Then $F'/[F', F]$ is free abelian on the set of $[x_i, x_j][F', F]$ where $i < j = 1, 2, \dots, n$ [*Hint*: If $n = 2$, show that $F/[F', F] \simeq U(3, \mathbb{Z})$ and deduce the result. In the general case assume a relation holds between the generators and apply a suitable endomorphism of F.]

15. Let F be the free group on $\{x, u\}$, and let $W = \langle x^2, u^2, [x, u]\rangle^F$. Show that F/W is a Klein 4-group, and then find a set of five free generators for N. [*Hint*: Choose the Schreier transversal $\{1, x, u, xu\}$.]

16. (P. Hall). There exists a finitely generated soluble group G which is not hopfian. [*Hint*: Let $N = U(3, \mathbb{Q}_2)$ where $\mathbb{Q}_2$ is the ring of rational numbers of the form $m2^n$, $(m, n \in \mathbb{Z})$. Let t be the diagonal matrix with diagonal entries, 1, 2, 1 and put $H = \langle t, N\rangle$. Denote by (a, b, c) the unitriangular matrix $1 + aE_{12} + bE_{23} + cE_{13}$ and write $u = (1, 0, 0)$, $v = (0, 1, 0)$, $w = (0, 0, 1)$. Prove that $H = \langle t, u, v\rangle$. Show also that the assignments $(a, b, c) \mapsto (a, 2b, 2c)$ and $t \mapsto t$ determine an automorphism of H; hence show that $H/\langle w\rangle \simeq H/\langle w^2\rangle$. Put $G = H/\langle w^2\rangle$.]

6.2. Free Products of Groups

Let there be given a nonempty set of groups $\{G_\lambda | \lambda \in \Lambda\}$. By a *free product* of the G_λ we mean a group G and a collection of homomorphisms $\iota_\lambda: G_\lambda \to G$ with the following mapping property. Given a set of homomorphisms $\varphi_\lambda: G_\lambda \to H$ into some group H, there is a *unique* homomorphism $\varphi: G \to H$ such that $\iota_\lambda \varphi = \varphi_\lambda$, that is, making all the diagrams below commute.



It is customary to suppress mention of the ι_λ, speaking of "the free product G."

From the category-theoretic point of view a free product is simply a coproduct in the category of groups (the product being the cartesian product—see Exercise 1.4.9).

Notice that the ι_λ are injective: this follows on taking H to be G_λ and φ_λ to be the identity function with $\varphi_\mu = 0$ if $\mu \neq \lambda$. We shall shortly see that the images of the ι_λ generate G. In a certain sense a free product is the "largest" group that can be generated by isomorphic copies of the G_λ (see Exercise 6.2.2).

The existence of free products is demonstrated by a construction similar to that used for free groups in Chapter 2. Before embarking on the construction we observe that free products, if they exist, are unique.

6.2.1. *If G and $\bar{G}$ are free products of a set of groups $\{G_\lambda | \lambda \in \Lambda\}$, then G and $\bar{G}$ are isomorphic.*

The proof, which is similar to that of 2.1.4, is left to the reader as an exercise.

Construction of the Free Product

6.2.2. *To every nonempty set of groups $\{G_\lambda | \lambda \in \Lambda\}$ there corresponds a free product.*

Proof. There is no loss of generality in assuming that $G_\lambda \cap G_\mu = \varnothing$ if $\lambda \neq \mu$ since G_λ can, if necessary, be replaced by an isomorphic copy. Let U be the union of all the G_λ, $\lambda \in \Lambda$. Consider the set S of all *words* in U, that is, all finite sequences

$$g = g_1 g_2 \cdots g_r$$

where $g_i \in G_{\lambda_i}$ and $\lambda_i \in \Lambda$. The *empty word* 1 is allowed, corresponding to the case $r = 0$. The *product gh* of two words is defined by juxtaposition, with the convention that $g1 = g = 1g$. The *inverse* of $g = g_1 g_2 \cdots g_r$ is defined to be $g_r^{-1} \cdots g_2^{-1} g_1^{-1}$, with the convention that $1^{-1} = 1$.

We define an equivalence relation $\sim$ on S in the following way: $g \sim h$ means that it is possible to pass from g to h by means of a finite sequence of operations of the following types:

(a) insertion of an identity element (of one of the groups G_λ);
(b) deletion of an identity element;
(c) contraction: replacement of two consecutive elements belonging to the same G_λ by their product;
(d) expansion: replacement of an element belonging to a G_λ by two elements of G_λ of which it is the product.

It should be clear that the relation $\sim$ is indeed an equivalence relation. Let G denote the set of all equivalence classes, the class containing g being written $[g]$.

One sees at once that $g \sim g'$ and $h \sim h'$ imply that $gh \sim g'h'$ and $g^{-1} \sim (g')^{-1}$. This permits us to give G the structure of a group by defining

$$[g][h] = [gh] \qquad \text{and} \qquad [g]^{-1} = [g^{-1}]:$$

the identity element is, of course, [1]. It is very easy to verify that the group axioms hold. The homomorphism $\iota_\lambda: G_\lambda \to G$ is defined by the rule $x^{\iota_\lambda} = [x]$, $x \in G_\lambda$.

Let us show that G and the ι_λ constitute a free product of the groups G_λ. To this end suppose we are given homomorphisms $\varphi_\lambda: G_\lambda \to H$ into some group H. Our task is to find a homomorphism $\varphi: G \to H$ such that $\iota_\lambda \varphi =$

φ_λ; there is a natural candidate,

$$[g]^\varphi = g_1^{\varphi_{\lambda_1}} \cdots g_r^{\varphi_{\lambda_r}},$$

where $g = g_1 \cdots g_n$ and $g_i \in G_{\lambda_i}$. To see that φ is well-defined observe that application of one of the operations (a)–(d) to g has no effect whatever on $g_1^{\varphi_{\lambda_1}} \cdots g_r^{\varphi_{\lambda_r}}$. This point being settled, it is obvious that φ is a homomorphism. If $x \in G_\lambda$, then $x^{\iota_\lambda \varphi} = [x]^\varphi = x^{\varphi_\lambda}$ by definition of φ; thus $\iota_\lambda \varphi = \varphi_\lambda$.

Finally suppose that $\varphi'\colon G \to H$ is another homomorphism with the property $\iota_\lambda \varphi' = \varphi_\lambda$. Then $\iota_\lambda \varphi = \iota_\lambda \varphi'$, so φ and φ' agree on Im ι_λ. But the Im ι_λ generate G; for if $g = g_1 g_2 \cdots g_r$ with $g_i \in G_{\lambda_i}$, then

$$[g] = [g_1][g_2] \cdots [g_r] = g_1^{\iota_1} g_2^{\iota_2} \cdots g_r^{\iota_r}$$

where $\iota_k = \iota_{\lambda_k}$. Hence $\varphi = \varphi'$. □

Notation. The free product G of the set of groups $\{G_\lambda | \lambda \in \Lambda\}$ will be written

$$G = \underset{\lambda \in \Lambda}{\mathrm{Fr}}\ G_\lambda.$$

By 6.2.1 this is unique up to isomorphism. The G_λ are called the *free factors* of G. If Λ is a finite set $\{\lambda_1, \ldots, \lambda_n\}$, it is usual to write

$$G = G_{\lambda_1} * G_{\lambda_2} * \cdots * G_{\lambda_n}.$$

Reduced Words

Let us return to the construction of the free product described in 6.2.2, with the object of obtaining a clearer picture of the form of its elements.

Let $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$. Call a word in $\bigcup_{\lambda \in \Lambda} G_\lambda$ *reduced* if none of its symbols is an identity and no two consecutive symbols belong to the same G_λ. It is agreed that the empty word 1 is reduced.

Starting with any word g, we can find by a canonical process a reduced word in the same equivalence class. First delete all identity elements occurring in g to obtain an equivalent word g'. Now consider a *segment* of g', by which is meant a subsequence of consecutive elements all belonging to the same G_λ which is not part of a longer subsequence of the same type. Replace each segment by the product of its elements to obtain a word g'' equivalent to g. The number of symbols of g'' is less than that of g unless g was reduced to begin with. The same procedure may be applied to g''. After a finite number of steps we reach a reduced word that is equivalent to g, say g^*.

Suppose that g and h are equivalent reduced words; we claim that $g = h$. To see this we introduce an action of the free product G on the set R of all reduced words. Let $u \in G_\lambda$; we define a permutation u' of R. If $u = 1_{G_\lambda}$, then $u' = 1$. Otherwise define u' by $(x_1 \cdots x_{r-1} x_r)u' = x_1 \cdots x_{r-1} x_r u$ or $x_1 \cdots x_{r-1}(x_r u)$ according as $\lambda \neq \lambda_r$ or $\lambda = \lambda_r$, with the stipulation that $x_r u$ is to be

deleted if it equals $1_{G_{\lambda_r}}$. Here of course $x_1 \cdots x_r \in R$ and $x_i \in G_{\lambda_i}$. Clearly $u \mapsto u'$ is a homomorphism from G_λ to $\mathrm{Sym}(R)$. By the defining property of free products these homomorphisms extend to a homomorphism $\theta: G \to \mathrm{Sym}(R)$. Let $g = y_1 \cdots y_s$ where $y_i \in G_{\lambda_i}$. Then $[g] = [y_1] \cdots [y_s]$ and $[g]^\theta = y_1' \cdots y_s'$. Thus $[g]^\theta$ sends the empty word 1 to g. Similarly $[h]^\theta$ sends 1 to h; hence $g = h$.

We have just proved the following basic result.

6.2.3. *Each equivalence class of words contains exactly one reduced word.*

Normal Form

Every element of the free product $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$ is of the form $[g]$ where g is a uniquely determined reduced word, say $g = g_1 g_2 \cdots g_r$ with $1 \neq g_i \in G_{\lambda_i}$. Then $\lambda_i \neq \lambda_{i+1}$ and

$$[g] = [g_1][g_2] \cdots [g_r]. \tag{3}$$

Let $\overline{G}_\lambda$ be the subgroup of all $[g]$ where $g \in G_\lambda$. Clearly $G_\lambda \simeq \overline{G}_\lambda$. Then in (3) we have $[g_i] \in \overline{G}_{\lambda_i}$. Every element of G has a unique expression as a product of elements of $\overline{G}_\lambda$, namely (3). This is called the *normal form* of g.

To achieve greater simplicity of notation it is usual to identify an x in G_λ with $[x]$ in $\overline{G}_\lambda$, so that G_λ becomes a subgroup of the free product. With this convention each element g of $\mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$ can be uniquely written in the form

$$g = g_1 g_2 \cdots g_r, \qquad (r \geq 0),$$

where $1 \neq g_i \in G_{\lambda_i}$ and $\lambda_i \neq \lambda_{i+1}$; the case $r = 0$ is interpreted as $g = 1$. Call the g_i the *syllables* of g and r the *length* of g as an element of the free product. Notice that $G_\lambda \cap \langle G_\mu | \lambda \neq \mu \in \Lambda \rangle = 1$.

The existence of a normal form is typical of free products in the following sense.

6.2.4. *Let G be a group generated by subgroups G_λ, $\lambda \in \Lambda$. Suppose that every element of G has a unique expression of the form $g_1 g_2 \cdots g_r$ where $r \geq 0$, $1 \neq g_i \in G_{\lambda_i}$, $\lambda_i \neq \lambda_{i+1}$. Then G is the free product of the G_λ's.*

This is easy to prove using the mapping property of the free product.

Examples of Free Products

Example I. *If F_λ is a free group of rank r_λ, then $F = \mathrm{Fr}_{\lambda \in \Lambda} F_\lambda$ is a free group of rank $\sum_{\lambda \in \Lambda} r_\lambda$. In particular, if each F_λ is infinite cyclic, F has rank $|\Lambda|$.*

For let F_λ be free on X_λ where the X_λ are disjoint sets. By 2.1.3 and the normal form in free products, F is free on $\bigcup_{\lambda \in \Lambda} X_\lambda$.

Example II. *The free product of two groups of order* 2 *is an infinite dihedral group.*

Let $G = \langle x \rangle * \langle y \rangle$ where $|x| = 2 = |y|$. Write $z = xy$. Then $G = \langle x, z \rangle$ and $z^x = z^{-1}$. Hence G is an image of an infinite dihedral group (by 2.2.1). Now a proper image of D_∞ is finite. On the other hand z has infinite order because $z, z^2, z^3, \ldots$ are distinct elements by uniqueness of normal form. Thus G is infinite dihedral.

A less obvious example of a free product is the projective special linear group $\mathrm{PSL}(2, \mathbb{Z})$ (see 3.2).

Example III. *The group* $\mathrm{PSL}(2, \mathbb{Z})$ *is the free product of a group of order* 2 *and a group of order* 3.

This result marked the first appearance of free products in the literature. It occurs with a geometric proof in work of Fricke and Klein [b23]. Free products were introduced as objects of study in group theory by Schreier in 1927.

Proof. Consider the elements

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

of $\mathrm{SL}(2, \mathbb{Z})$. Let $H = \langle A, B \rangle$. We show first that $H = \mathrm{SL}(2, \mathbb{Z})$. If this is false, choose an element of $\mathrm{SL}(2, \mathbb{Z}) \backslash H$

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $|a| + |c|$ minimal. For the moment suppose that $a \neq 0$ and $c \neq 0$. Now $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and

$$(AB)^r X = \begin{pmatrix} a + rc & b + rd \\ c & d \end{pmatrix} \notin H.$$

If $|a| \geq |c|$, the integer r can be chosen so that $|a + rc| < |a|$; then $|a + rc| + |c| < |a| + |c|$, contradicting the choice of X. Hence $|a| < |c|$. In this case an integer s can be found such that $|sa + c| < |c|$; however

$$(BA)^{-s} X = \begin{pmatrix} a & b \\ sa + c & sb + d \end{pmatrix} \notin H.$$

Therefore $a = 0$ or $c = 0$. In the first case $X = \begin{pmatrix} 0 & 1 \\ -1 & d \end{pmatrix}$ or $\begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}$ and $B^{-1}X$ equals $A^2(AB)^{-d-1}$ or $(AB)^{d-1}$ respectively. If $c = 0$, then $X = (AB)^b$ or $A^2(AB)^{-b}$, a final contradiction. Hence A and B generate $\mathrm{SL}(2, \mathbb{Z})$.

Let $\bar{A}$ and $\bar{B}$ be the images of A and B under the natural homomorphism $SL(2, \mathbb{Z}) \to PSL(2, \mathbb{Z})$. Since $A^2 = -1 = B^3$, we see that $|\bar{A}| = 2$ and $|\bar{B}| = 3$. Let $\langle a \rangle$ and $\langle b \rangle$ be groups of order 2 and 3 respectively and write $G = \langle a \rangle * \langle b \rangle$. By the mapping property of the free product, the assignments $a \mapsto \bar{A}$, $b \mapsto \bar{B}$ determine a surjective homomorphism $\varphi: G \to PSL(2, \mathbb{Z})$. To complete the proof one shows that $\operatorname{Ker} \varphi = 1$.

Let $x \in \operatorname{Ker} \varphi$. Then we can assume that x is a product of ab's and ab^{-1}'s with a possible initial $b^{\pm 1}$ or a final a (but not both). However

$$(AB)^r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad (AB^{-1})^s = (-1)^s \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix},$$

where $r, s \geq 0$. Thus a nonempty product of such elements cannot contain both positive and negative entries, and therefore cannot equal $\pm A$ or $\pm B^{\pm 1}$. It follows that $x = 1$. □

Elementary Properties of Free Products

Elements of finite order in a free product are subject to severe restrictions.

6.2.5. *Let $G = \operatorname{Fr}_{\lambda \in \Lambda} G_\lambda$.*

(i) *Let $g_1 g_2 \cdots g_n$ be the normal form of an element g of G. If the syllables g_1 and g_n belong to different free factors, then g has infinite order.*
(ii) *If at least two free factors are nontrivial, then G contains an element of infinite order.*
(iii) *An element of G with finite order is conjugate to an element in one of the free factors.*

Proof. (i) By uniqueness of normal form g^m cannot equal 1 for any $m > 0$.

(ii) This follows from (i).

(iii) Suppose that g has finite order and let $g = g_1 g_2 \cdots g_n$ be the normal form. Certainly we can assume that $n > 1$. Then g_1 and g_n must both belong to the same free factor G_λ by (i), and $n > 2$. But the element $g^{g_n^{-1}} = (g_n g_1) g_2 \cdots g_{n-1}$ also has finite order. In view of (i) this is a contradiction. □

In particular *a free product of torsion-free groups is torsion-free.*

6.2.6. *Let $G = \operatorname{Fr}_{\lambda \in \Lambda} G_\lambda$. If $1 \neq g \in G_\lambda$, then $C_G(g)$ is contained in G_λ.*

Proof. Let $x \in C_G(g)$ and write $x = x_1 x_2 \cdots x_n$, the normal form. If x_1 and x_n both belong to G_λ, replace x by $x^{x_n^{-1}}$, which belongs to $C_G(g^{x_n^{-1}})$. So we can assume that x_1 and x_n do not both belong to G_λ. But then $g x_1 x_2 \cdots x_n = x_1 x_2 \cdots x_n g$, which can only mean that $n = 1$ and $x = x_1 \in G_\lambda$. □

An immediate consequence is that *the center of a free product is trivial if at least two of the free factors are nontrivial.*

6.2.7. *Let $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$ and $H = \mathrm{Fr}_{\lambda \in \Lambda} H_\lambda$ be free products. Let there be given homomorphisms $\varphi_\lambda: G_\lambda \to H_\lambda$. Then there is a unique homomorphism φ: $G \to H$ whose restriction to G_λ is φ_λ. Furthermore the kernel of φ is the normal closure in G of $\bigcup_{\lambda \in \Lambda} \mathrm{Ker}\, \varphi_\lambda$.*

Proof. The existence and uniqueness of φ follow from the mapping property of the free product. Let N denote the normal closure of $\bigcup_{\lambda \in \Lambda} \mathrm{Ker}\, \varphi_\lambda$ and write $K = \mathrm{Ker}\, \varphi$. Since φ_λ is the restriction of φ to G_λ, we have $N \leq K$. Suppose that g is an element of shortest length in $K \backslash N$. Let $g = g_1 g_2 \cdots g_r$ be the normal form with $g_i \in G_{\lambda_i}$. Now $1 = g^\varphi = g_1^{\varphi_{\lambda_1}} g_2^{\varphi_{\lambda_2}} \cdots g_r^{\varphi_{\lambda_r}}$ and $g_i^{\varphi_{\lambda_i}} \in H_{\lambda_i}$. By uniqueness of normal form in H some $g_i^{\varphi_{\lambda_i}} = 1$ and $g_i \in N$. Hence $g_1 \cdots g_{i-1} g_{i+1} \cdots g_r \in K \backslash N$, in contradiction to the choice of g. □

Exercises 6.2

1. Prove 6.2.1 (the uniqueness of free products).
2. If a group G is generated by subgroups G_λ, $\lambda \in \Lambda$, then G is an image of $\mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$.
3. Given a family of groups $\{G_\lambda | \lambda \in \Lambda\}$, find a natural epimorphism from $\mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$ to $\mathrm{Dr}_{\lambda \in \Lambda} G_\lambda$ and identify its kernel.
4. Prove that $(\mathrm{Fr}_{\lambda \in \Lambda} G_\lambda)_{\mathrm{ab}} \simeq \mathrm{Dr}_{\lambda \in \Lambda} (G_\lambda)_{\mathrm{ab}}$.

*5. Let $N_\lambda \lhd G_\lambda$ and write N for normal closure of $\bigcup_{\lambda \in \Lambda} N_\lambda$ in $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$. Prove that $G/N \simeq \mathrm{Fr}_{\lambda \in \Lambda}(G_\lambda / N_\lambda)$.

6. Let $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$ and let H_λ be a subgroup of G_λ. If H is the subgroup of G generated by the H_λ, show that $H \simeq \mathrm{Fr}_{\lambda \in \Lambda} H_\lambda$.
7. Let $G = H * K$ where $H \neq 1$ and $K \neq 1$. Prove that $[H, K]$ is a free group on the set of elements $[h, k]$ where $1 \neq h \in H$ and $1 \neq k \in K$. What is the rank of $[H, K]$? [*Hint*: Let $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_r}^{\varepsilon_r}$ be a reduced word in some set X. Let w' be the element of G obtained when x_{i_j} is replaced by $[h_j, k_j]$ where the (h_j, k_j) are distinct pairs of nontrivial elements from H and K. Show by induction on r that the normal form of w' ends in $h_r k_r$ or $k_r h_r$.]
8. Prove that $\mathrm{PSL}(2, \mathbb{Z})'$ is a free group of rank 2.
9. Let $G = \langle x, y | x^r = 1 = y^s \rangle$ where $r, s \geq 0$. If $G = \langle (x^t)^g, y \rangle$ where $g \in G$ and t is positive integer, show that g has the form $x^k y^l$.
10. Let $G = \langle x, y | x^r = 1 = y^s \rangle$ where $r \neq s$. If $\gamma \in \mathrm{Aut}\, G$, prove that $x^\gamma = (x^i)^g$ and $y^\gamma = (y^j)^g$ where $g \in G$ and $(i, r) = 1 = (j, s)$. [*Hint*: Use 6.2.5(iii) and the preceding exercise.] Deduce that $\mathrm{Out}\, G \simeq \mathbb{Z}_r^* \times \mathbb{Z}_s^*$.
11. Prove that $\mathrm{Aut}(\mathrm{PSL}(2, \mathbb{Z})) \simeq \mathrm{PGL}(2, \mathbb{Z})$.

12. Let $G = \langle x, y | x^r = 1 = y^r \rangle$. If $\gamma \in \mathrm{Aut}\, G$, prove that either $x^\gamma = (x^i)^g$ and $y^\gamma = (y^i)^g$ or $x^\gamma = (y^j)^g$ and $y^\gamma = (x^j)^g$ where $g \in G$ and $(i, r) = 1 = (j, r)$. Deduce that $\mathrm{Out}\, G \simeq \mathbb{Z}_r^* \rtimes \mathbb{Z}_2$.

13. Prove 6.2.4 (the existence of a normal form characterizes free products).

6.3. Subgroups of Free Products

There is a famous and fundamental theorem of Kuroš which describes the structure of subgroups of a free product.

6.3.1 (The Kuroš Subgroup Theorem). *Let H be a subgroup of the free product $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$. Then H is a free product of the form*

$$H = H_0 * \mathop{\mathrm{Fr}}_{\lambda, d_\lambda} H \cap (d_\lambda G_\lambda d_\lambda^{-1}),$$

where H_0 is a free group, d_λ varies over a set of (H, G_λ)-double coset representatives and λ varies over Λ.

Furthermore, if H has finite index m in G, the rank of the free group H_0 is $\sum_{\lambda \in \Lambda} (m - m_\lambda) + 1 - m$ where m_λ is the number of (H, G_λ)-double cosets in G.

Let us examine the statement of this theorem in the case where each G_λ is infinite cyclic, so that G is a free group. The first assertion is that any subgroup H is free. Suppose that $|G : H| = m$ is finite; thus so is m_λ. Let $G_\lambda = \langle x_\lambda \rangle$ and let d_λ be an (H, G_λ)-double coset representative. For a fixed λ all the cosets $Hd_\lambda x_\lambda^r$ cannot be distinct. Hence $Hd_\lambda = Hd_\lambda x_\lambda^r$ for some $r > 0$. Thus $d_\lambda x_\lambda^r = hd_\lambda$ where $h \in H$, from which it follows that $1 \neq h \in H \cap (d_\lambda G_\lambda d_\lambda^{-1})$; the latter group is therefore infinite cyclic. Hence the rank of H is equal to that of H_0 plus $\sum_{\lambda \in \Lambda} m_\lambda$, which equals $nm + 1 - m$ where $n = |\Lambda|$. Thus the Nielsen–Schreier Theorem is a consequence of the Kuroš Subgroup Theorem.

In proving 6.3.1 we follow once again the method of A.J. Weir, making use of coset maps. It is important to realize that the proof is basically similar to that of the Nielsen–Schreier Theorem, although the details are necessarily more complicated.

Consider the situation of 6.3.1. For each λ in Λ choose a presentation $\varphi_\lambda : F_\lambda \to G_\lambda$ with F_λ free. By 6.2.7 the φ_λ determine an epimorphism φ from $F = \mathrm{Fr}_{\lambda \in \Lambda} F_\lambda$ to $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$. Let W be the preimage of H under φ. If a presentation of W is given, composition with φ yields a presentation of H. It will turn out that such a presentation of W can be found which elucidates the structure of H as a free product. It is for this reason that we begin by investigating subgroups of F.

Subgroups of Free Products of Free Groups

Let F be the free product of free groups

$$F = \underset{\lambda \in \Lambda}{\mathrm{Fr}}\ F_\lambda,$$

F_λ being free on a set X_λ. Let W be a subgroup of F, which will be fixed from now on. The right cosets of W are labeled by an index set I containing the symbol 1,

$$\{W_i \mid i \in I\},$$

where $W = W_1$.

For each λ in Λ we choose a right transversal to W in F, the λ-representative of the coset W_i being written

$$^{\lambda}\overline{W_i}.$$

At present we require only that $^{\lambda}\overline{W} = 1$ for all λ. A more careful choice of transversals will be made later.

Our immediate object is to construct a presentation of W. With each i in I and x in $\bigcup_{\lambda \in \Lambda} X_\lambda$ we associate a symbol y_{ix}. The idea is to assign to y_{ix} the element $^{\lambda}\overline{W_i}x(^{\lambda}\overline{W_i x})^{-1}$ of W. However the free group on the set of y_{ix}'s is not large enough to present W, as it turns out; so we add some more symbols.

Choose any element of Λ and call it 1: it is to remain fixed throughout the proof. With each pair (i, λ) where $1 \neq i \in I$ and $1 \neq \lambda \in \Lambda$ we associate a symbol $z_{i\lambda}$. Now define

$$\hat{F}$$

to be the free group on the set of all y_{ix} and $z_{i\lambda}$.

We construct a homomorphism

$$\tau\colon \hat{F} \to W$$

by means of the assignments

$$y_{ix} \mapsto {}^{\lambda}\overline{W_i}x(^{\lambda}\overline{W_i x})^{-1} \qquad \text{and} \qquad z_{i\lambda} \mapsto {}^{\lambda}\overline{W_i}(^{1}\overline{W_i})^{-1},$$

where $x \in X_\lambda$. It will be shown that τ is an epimorphism; thus τ leads to a presentation of W in the y_{ix} and $z_{i\lambda}$.

To save endless qualification let us agree that

$$z_{1\lambda} = 1 = z_{i1}$$

for all λ and i.

Coset Maps

For each u in F and i in I we define an element u^{W_i} of $\hat{F}$ recursively by induction on the length of u as a reduced word in $\bigcup_{\lambda \in \Lambda} X_\lambda$. In the first

place

$$1^{W_i} = 1, \qquad x^{W_i} = y_{ix}, \qquad \text{and} \qquad (x^{-1})^{W_i} = (x^{W_i x^{-1}})^{-1}$$

if $x \in \bigcup_{\lambda \in \Lambda} X_\lambda$. Let $u = vy$ where $v \neq 1$ and $y \in X_\mu \cup X_\mu^{-1}$ is the final symbol of u in the normal form: then we define

$$u^{W_i} = v^{W_i}(z_{j\lambda} z_{j\mu}^{-1}) y^{W_j},$$

where $W_j = W_i v$ and the final syllable of v belongs to F_λ. (The last statement will henceforth be rendered *v ends in λ*: similarly *v begins in ν* if the first syllable of v belongs to F_ν.) The mapping

$$u \mapsto u^{W_i} \qquad (u \in F),$$

is called a *coset map*. Apart from the factor zz^{-1}, the definition is the same as in the proof of the Nielsen–Schreier Theorem.

We proceed to compute the effect of a coset map on products and inverses.

6.3.2. *Let u and v be elements of F.*

(i) *If neither u nor v cancels completely in the product uv, then*

$$(uv)^{W_i} = u^{W_i} z_{j\lambda} z_{j\mu}^{-1} v^{W_j},$$

where $W_j = W_i u$, u ends in λ, and v beings in μ.

(ii) $(u^{-1})^{W_i} = (u^{W_i u^{-1}})^{-1}$.

Proof. Write v as a reduced word in $\bigcup_{\lambda \in \Lambda} X_\lambda$. The proof of (i) is by induction on l, the length of v as a reduced word: note that $l > 0$, otherwise we consider v to have canceled. If $l = 1$, then $v \in X_\lambda \cup X_\lambda^{-1}$ for some λ and (i) is true by definition. Assume that $l > 1$ and write $v = v_1 y$ where $y \in X_\nu \cup X_\nu^{-1}$ is the final symbol of v. Then $uv = (uv_1)y$. Observe that u does not cancel completely in uv_1; assume that v_1 does not cancel completely either. By definition

$$(uv)^{W_i} = (uv_1)^{W_i} z_{k\rho} z_{k\nu}^{-1} y^{W_k},$$

where $W_k = W_i u v_1$ and uv_1 ends in ρ: thus v_1 ends in ρ. By induction on l

$$(uv_1)^{W_i} = u^{W_i} z_{j\lambda} z_{j\mu}^{-1} v_1^{W_j}.$$

Hence

$$\begin{aligned}(uv)^{W_i} &= (u^{W_i} z_{j\lambda} z_{j\mu}^{-1} v_1^{W_j})(z_{k\rho} z_{k\nu}^{-1}) y^{W_k} \\ &= u^{W_i} z_{j\lambda} z_{j\mu}^{-1} (v_1 y)^{W_j} \\ &= u^{W_i} z_{j\lambda} z_{j\mu}^{-1} v^{W_j}.\end{aligned}$$

In particular the product rule holds if no cancellation between u and v occurs. Using this fact it is easy to prove (ii) by induction on the length of u.

Now suppose that v_1 cancels completely in uv_1. Then the final part of u is v_1^{-1} and $u = u_1 v_1^{-1}$ for some u_1 (without cancellation). Note that y does not

cancel in $uv = u_1 y$. Also $u \neq 1$, otherwise u would cancel completely. Hence

$$(uv)^{W_i} = (u_1 y)^{W_i} = u_1^{W_i} z_{l\sigma} z_{l\nu}^{-1} y^{W_l}, \tag{4}$$

where $W_l = W_i u_1$ and u_1 ends in σ. The product rule holds for $u = u_1 v_1^{-1}$ by what has already been proved. Thus

$$u^{W_i} = u_1^{W_i} z_{l\sigma} z_{l\rho}^{-1} (v_1^{-1})^{W_l}, \tag{5}$$

where v_1 ends in ρ. By (ii) we have $(v_1^{-1})^{W_l} = (v_1^{W_l v_1^{-1}})^{-1} = (v_1^{W_j})^{-1}$ since $W_l v_1^{-1} = W_i u = W_j$. Substitute for $u_1^{W_i}$ in (4) using (5): we obtain

$$\begin{aligned}(uv)^{W_i} &= u^{W_i} v_1^{W_j} z_{l\rho} z_{l\sigma}^{-1} (z_{l\sigma} z_{l\nu}^{-1} y^{W_l}) \\ &= u^{W_i} (v_1 y)^{W_j} = u^{W_i} v^{W_j},\end{aligned}$$

the correct answer because $\lambda = \mu$ when cancellation occurs between u and v. □

Simple examples show that the product rule does not hold in general (Exercise 6.3.9), a fact that complicates some proofs. Two further instances when the rule is valid are useful.

6.3.3.

(i) *If $u, v \in F$ and $uv \in W$, then $(uv)^W = u^W z_{i\lambda} z_{i\mu}^{-1} v^{W_i}$ where $W_i = Wu$, u ends in λ, and v begins in μ.*
(ii) *If $u, v \in F_\lambda$, then $(uv)^{W_i} = u^{W_i} v^{W_i u}$.*

Proof. (i) If neither u nor v cancels completely, the equation is already known. Suppose that v cancels completely and $u = u_1 v^{-1}$ in reduced form. Then $uv = u_1 \in W$ and $(uv)^W = u_1^W$. From $u = u_1 v^{-1}$ and 6.3.2 we obtain $u^W = u_1^W (v^{-1})^W$ since $Wu_1 = W$ and $z_{1\nu} = 1$ for all ν. Hence $u_1^W = u^W((v^{-1})^W)^{-1} = u^W v^{W_i}$ since $Wv^{-1} = Wu = W_i$. Thus $(uv)^W = u^W v^{W_i}$, which is correct because $\lambda = \mu$ in this case. If u cancels completely, the argument is similar.

(ii) We leave the proof as an exercise. □

If $u, v \in W$, then 6.3.3(i) yields $(uv)^W = u^W v^W$ since $z_{1\lambda} = 1 = z_{1\mu}$. Hence the mapping $u \mapsto u^W$ is a homomorphism; we shall call this

$$\psi: W \to \hat{F}.$$

We investigate next the effect of composing ψ with τ.

6.3.4. *If $1 \neq u \in F$, then $(u^{W_i})^\tau = {}^\lambda\overline{W_i}u({}^\mu\overline{W_i u})^{-1}$ where u begins in λ and ends in μ.*

Proof. Let $u = vy$ in reduced form where $y \in X_\mu \cup X_\mu^{-1}$. We can also assume $v \neq 1$; otherwise the result follows from the definitions of y^{W_i} and $(y^{-1})^{W_i}$.

By 6.3.2

$$u^{W_i} = (vy)^{W_i} = v^{W_i} z_{jv} z_{j\mu}^{-1} y^{W_j},$$

where $W_j = W_i v$ and v ends in v. By induction on the length of u as a word in $\bigcup_{\lambda \in \Lambda} X_\lambda$,

$$(u^{W_i})^\tau = {}^\lambda\overline{W_i}v({}^v\overline{W_j})^{-1} \cdot {}^v\overline{W_j}\,{}^1\overline{W_j}^{-1} \cdot ({}^\mu\overline{W_j}\,{}^1\overline{W_j}^{-1})^{-1} \cdot {}^\mu\overline{W_j}y({}^\mu\overline{W_j y})^{-1},$$

which becomes after cancellation

$$(u^{W_i})^\tau = {}^\lambda\overline{W_i}vy({}^\mu\overline{W_i u})^{-1} = {}^\lambda\overline{W_i}u({}^\mu\overline{W_i u})^{-1}. \qquad \square$$

If $u \in W$ and $i = 1$, the formula of 6.3.4 yields $(u^W)^\tau = {}^\lambda\overline{W}u({}^\mu\overline{W})^{-1} = u$. Therefore

$$\psi\tau = 1.$$

It follows that ψ is injective and τ surjective. Write

$$\chi = \tau\psi,$$

which is an endomorphism of $\hat{F}$ satisfying $\chi^2 = \chi$.

We proceed to find a set of generators and relators for the presentation $\tau: \hat{F} \to W$.

6.3.5. *The group W has a presentation $\tau: \hat{F} \to W$ with generators y_{ix}, $z_{i\lambda}$ and relators*

$$y_{ix}^{-1} y_{ix}^{\chi} \qquad \textit{and} \qquad z_{i\lambda}^{-1} z_{i\lambda}^{\chi},$$

where $i \in I$, $\lambda \in \Lambda$, $x \in \bigcup_{\lambda \in \Lambda} X_\lambda$.

Proof. Let $K = \operatorname{Ker} \tau$. Since $\chi = \tau\psi$ and ψ is injective, $K = \operatorname{Ker} \chi$. Let N denote the normal closure in $\hat{F}$ of the set of all $y_{ix}^{-1} y_{ix}^{\chi}$ and $z_{i\lambda}^{-1} z_{i\lambda}^{\chi}$. Then, since $\chi = \chi^2$, we have $N \leq K$. On the other hand, any k in K is expressible in terms of y_{ix} and $z_{i\lambda}$, so $1 = k^\chi \equiv k \bmod N$. Therefore $k \in N$ and $N = K$. $\square$

Kuroš Systems of Transversals

The time has come to make a careful choice of transversals. It is convenient to do this in the more general context of a subgroup H of an arbitrary free product $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$. A set of λ-transversals to H, say $\{{}^\lambda\overline{H_i} \mid i \in I\}$, $\lambda \in \Lambda$, with right cosets H_i of H, is called a *Kuroš system of transversals* if there exists for each λ a set of (H, G_λ)-double coset representatives d_λ such that the following hold:

K(i) d_λ is an element of shortest length (in the free product) in its (H, G_λ)-double coset D.
K(ii) If $H_i \subseteq D$, then ${}^\lambda\overline{H_i} \in d_\lambda G_\lambda$.
K(iii) If d_λ ends in μ, then $\mu \neq \lambda$ and ${}^\mu\overline{Hd_\lambda} = d_\lambda$.
K(iv) ${}^\lambda\overline{Hd_\lambda} = d_\lambda$.

We shall see in 6.3.6 that such a set of transversals always exists. By choosing a Kuroš set of transversals a more economical set of relators is obtained. Notice the similarity of K(ii) to the Schreier property.

Let us now establish the existence of a set of transversals with the Kuroš properties.

6.3.6. *Corresponding to any subgroup H of a free product $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$ there exists a Kuroš system of transversals.*

Proof. Let 1 be the representative of the double coset HG_λ. If $H_i \subseteq HG_\lambda$, choose for ${}^\lambda\overline{H}_i$ an element of G_λ. So far all conditions have been met. Let D be an (H, G_λ)-double coset of length l, that is to say, l is the length of a shortest element d' of D. Assume that coset representatives have been chosen appropriately for all double cosets of length less than l and that transversal elements have been assigned to cosets of H contained in such double cosets. Now $D = Hd'G_\lambda$ and d' cannot end in λ by minimality of length—suppose that d' ends in μ. Then $Hd'G_\mu$ has length less than l, so its representative d'', as well as ${}^\mu\overline{Hd'}$, has already been assigned: put $d = {}^\mu\overline{Hd'}$. Now the length of d'' is at most $l - 1$. In addition $d \in d''G_\mu$ by K(ii), so the length of d is at most l (and hence equals l). Choose this d to be the representative of D, noting that K(i) and K(iii) hold. If H_i is contained in D, we simply define the ${}^\lambda\overline{H}_i$ so as to satisfy K(ii) and K(iv). In this way we construct recursively a Kuroš system of transversals. □

Reassured that such sets of transversals always exist, we return to the subgroup W of $F = \mathrm{Fr}_{\lambda \in \Lambda} F_\lambda$.

6.3.7. *If a Kuroš system of transversals to W is chosen, the following elements constitute a set of relators for $\tau: \hat{F} \to W$: the u^W where u is a nontrivial element of a transversal and the $z_{j\lambda} z_{j\mu}^{-1}$ where ${}^\lambda\overline{W}_j = {}^\mu\overline{W}_j$.*

Proof. Let $K = \mathrm{Ker}\, \tau$ and denote by N the normal closure in $\hat{F}$ of the set of potential relators. We show first that $N \leq K$. Let $u = {}^\lambda\overline{W}_i$ and suppose that $W_i = Wu \subseteq D = WdF_\lambda$ where d is the representative of D. Then by 6.3.4

$$(u^W)^\tau = {}^\nu\overline{Wu}({}^\mu\overline{Wu})^{-1} = u({}^\mu\overline{W}_i)^{-1}$$

where u begins in ν and ends in μ. If $\mu = \lambda$, then $u = {}^\mu\overline{W}_i$. If $\mu \neq \lambda$, then, since $u \in dF_\lambda$ by K(ii), we have $u = d$: note that d does not end in λ. Thus ${}^\mu\overline{W}_i = {}^\mu\overline{Wd} = d$ by K(iii). Hence in both cases $u = {}^\mu\overline{W}_i$ and $(u^W)^\tau = 1$.

Next, if $z_{j\lambda} z_{j\mu}^{-1}$ is one of the specified relators,

$$(z_{j\lambda} z_{j\mu}^{-1})^\tau = ({}^\lambda\overline{W}_j\, {}^1\overline{W}_j^{-1})({}^\mu\overline{W}_j\, {}^1\overline{W}_j^{-1})^{-1} = {}^\lambda\overline{W}_j\, {}^\mu\overline{W}_j^{-1} = 1.$$

Hence $N \leq K$.

It remains to show that $K \leq N$ or, equivalently, that $y_{ix}^\chi \equiv y_{ix} \bmod N$ and $z_{i\lambda}^\chi \equiv z_{i\lambda} \bmod N$ (by 6.3.5).

First of all consider

$$y_{ix}^{\chi} = ({}^{\lambda}\overline{W_i}x\,{}^{\lambda}\overline{W_i x}^{-1})^W = (uxv^{-1})^W \tag{6}$$

where $x \in X_\lambda$, $u = {}^{\lambda}\overline{W_i}$, and $v = {}^{\lambda}\overline{W_i x}$. Now $W_i \subseteq WdF_\lambda$ for some double coset representative d. Thus $u \in dF_\lambda$ and $v \in dF_\lambda$ by K(ii), and we may write $u = df$ and $v = dg$ where $f, g \in F_\lambda$. Therefore, by the product rule, (6) becomes

$$\begin{aligned} y_{ix}^{\chi} &= (d(fxg^{-1})d^{-1})^W \\ &= d^W z_{j\mu} z_{j\lambda}^{-1} (fxg^{-1})^{W_j} z_{j\lambda} z_{j\mu}^{-1} (d^W)^{-1} \end{aligned}$$

where $W_j = Wd = Wdfxg^{-1}$ and d ends in μ; here we have assumed that $fxg^{-1} \neq 1$. Now ${}^{\lambda}\overline{W_j} = d = {}^{\mu}\overline{W_j}$ by K(iii) and K(iv). Hence

$$y_{ix}^{\chi} \equiv (fxg^{-1})^{W_j} \mod N.$$

Notice that this is true even if $fxg^{-1} = 1$. Next using 6.3.3(ii) we obtain

$$y_{ix}^{\chi} \equiv f^{W_j} x^{W_i} (g^{W_j})^{-1} \mod N.$$

Since $y_{ix} = x^{W_i}$, it is enough to show that f^{W_j} and $g^{W_j} \in N$. Assume that $f \neq 1$: then we deduce from $u = df$ that $u^W = d^W z_{j\mu} z_{j\lambda}^{-1} f^{W_j}$, which implies that $f^{W_j} \in N$. Similarly $g^{W_j} \in N$.

The relator $z_{i\lambda}^{-1} z_{i\lambda}^{\chi}$ is handled in a similar way; the details are left as an exercise for the reader. □

We shall now partition the y_{ix} in a manner corresponding to the decomposition of F into double cosets. Let $\lambda \in \Lambda$ and let d be the representative of a (W, F_λ)-double coset D. Define

$$\hat{F}_{\lambda d} = \langle y_{ix} \mid W_i \subseteq D, x \in X_\lambda \rangle.$$

Each y_{ix} belongs to exactly one $\hat{F}_{\lambda d}$. If Z is the subgroup generated by all the $z_{i\lambda}$, then

$$\hat{F} = Z * \operatorname*{Fr}_{\lambda, d_\lambda} \hat{F}_{\lambda, d_\lambda}; \tag{7}$$

here d_λ ranges over all (W, F_λ)-double coset representatives and $\lambda \in \Lambda$. We shall find a set of relators for $\tau: \hat{F} \to W$ each of which belongs to a free factor of (7).

6.3.8. *The presentation $\tau: \hat{F} \to W$ has a set of defining relators consisting of the elements of $\hat{F}_{\lambda, d_\lambda} \cap \operatorname{Ker} \tau$ and all $z_{j\lambda} z_{j\mu}^{-1}$ where ${}^{\lambda}\overline{W_j} = {}^{\mu}\overline{W_j}$.*

Proof. Let N be the normal closure in $\hat{F}$ of the specified set of elements. Then $N \leq K = \operatorname{Ker} \tau$ by 6.3.7. Furthermore by the same result it is enough to prove that $u^W \in N$ where u is a λ-transversal element. Assuming this to be false, we can find a (W, F_λ)-double coset D of minimal length subject to the existence of a coset W_i contained in D whose representative $u = {}^{\lambda}\overline{W_i}$ does not satisfy $u^W \in N$.

By K(ii) we may write $u = df$ where $f \in F_\lambda$ and d is a double coset representative of D. Then

$$u^W = d^W(z_{j\mu}z_{j\lambda}^{-1})f^{W_j} \tag{8}$$

where $W_j = Wd$ and d ends in $\mu \neq \lambda$. The length of the double coset WdF_μ is less than that of d; hence it is less than the length of $D = WdF_\lambda$ by K(i). Also ${}^\mu\overline{Wd} = d$ by K(iii), so $d^W \in N$ by minimality. Now ${}^\mu\overline{Wd} = {}^\lambda\overline{Wd}$ by K(iii) and K(iv); hence $z_{j\mu}z_{j\lambda}^{-1} \in N$ and it suffices to deal with f^{W_j}. By (8) we have $f^{W_j} \in K$. Thus it is enough to prove the following statement: if $f \in F_\lambda$, then

$$f^{W_l} \in \hat{F}_{\lambda d} \tag{9}$$

whenever $W_l \subseteq WdF_\lambda$. If $f \in X_\lambda$, then $f^{W_l} = y_{lf}$, which belongs to $\hat{F}_{\lambda d}$ by definition: if $f \in X_\lambda^{-1}$, then $f^{W_l} = y_{mf^{-1}}^{-1} \in \hat{F}_{\lambda d}$ where $W_m = W_l f^{-1}$. In the general case write f as a reduced word in X_λ and induct on its length. □

This set of relators enables us to recognize the free product structure of W.

6.3.9. *Let W be a subgroup of $F = \mathrm{Fr}_{\lambda\in\Lambda} F_\lambda$, the F_λ being free groups. Then there exists for each λ in Λ a set of (W, F_λ)-double coset representatives $\{d_\lambda\}$ such that there is a free product decomposition*

$$W = W_0 * \mathop{\mathrm{Fr}}_{\lambda, d_\lambda} W \cap (d_\lambda F_\lambda d_\lambda^{-1})$$

where W_0 is a free group and the free product is formed over all double cosets $Wd_\lambda F_\lambda$ and all λ in Λ. Furthermore, should $|F : W| = m$ be finite, the rank of the free group W_0 is

$$\sum_{\lambda\in\Lambda} (m - m_\lambda) + 1 - m$$

where m_λ is the number of (W, F_λ)-double cosets in F.

Proof. We assume of course that a Kuroš system of transversals and double coset representatives for W has been selected. According to 6.3.8 the presentation $\tau: \hat{F} \to W$ has a set of defining relators each of which belongs to $Z = \langle Z_{i\lambda} | i \in I, \lambda \in \Lambda \rangle$ or to one of the $\hat{F}_{\lambda d}$, that is, to one of the free factors in (7). By Exercise 6.2.5 the subgroup W is the free product of $W_0 = Z^\tau$ and the $\hat{F}_{\lambda d}^\tau$. We claim that

$$\hat{F}_{\lambda d}^\tau = W \cap (dF_\lambda d^{-1}). \tag{10}$$

To see this take any y_{ix} in $\hat{F}_{\lambda d}$; then $y_{ix}^\tau = {}^\lambda\overline{W_i}x({}^\lambda\overline{W_i x})^{-1}$ where $x \in X_\lambda$. Now $W_i \subseteq WdF_\lambda$ by definition of $\hat{F}_{\lambda d}$, so ${}^\lambda\overline{W_i} = df$ for some $f \in F_\lambda$: also $W_i x \subseteq WdF_\lambda$ and ${}^\lambda\overline{W_i x} = dg$ where $g \in F_\lambda$. Hence

$$y_{ix}^\tau = (df)x(dg)^{-1} = d(fxg^{-1})d^{-1} \in W \cap (dF_\lambda d^{-1}).$$

Thus $\hat{F}_{\lambda d}^\tau \leq W \cap (dF_\lambda d^{-1})$.

To establish the converse we choose $w \neq 1$ from $W \cap (dF_\lambda d^{-1})$. Since $w = w^{\psi\tau} = (w^W)^\tau$, it will suffice to prove that $w^W \in \hat{F}_{\lambda d}K$, where as usual $K = \operatorname{Ker} \tau$. Write $w = dfd^{-1}$ with $1 \neq f \in F_\lambda$. Note that d ends in some $\mu \neq \lambda$. Also $Wdf = Wd = W_j$ say. By the product rule

$$w^W = (dfd^{-1})^W = d^W z_{j\mu} z_{j\lambda}^{-1} f^{W_j} z_{j\lambda} z_{j\mu}^{-1} (d^{-1})^{W_j}.$$

Since $(d^{-1})^{W_j} = (d^W)^{-1}$, it follows that

$$w^W \equiv f^{W_j} \mod K.$$

But $f^{W_j} \in \hat{F}_{\lambda d}$ by (9), so $w^W \in \hat{F}_{\lambda d}K$ as required.

It remains to discuss $W_0 = Z^\tau$. The relators which affect Z are the $z_{j\lambda} z_{j\mu}^{-1}$, $j \neq 1$, $\lambda \neq \mu$, each of which eliminates one of the z's. Hence W_0 is free. Now let $|F : W| = m$ be finite; the rank of W_0 has to be computed.

An element $z_{j\lambda} z_{j\mu}^{-1}$ belongs to K if and only if ${}^\lambda\overline{W}_j = {}^\mu\overline{W}_j$. Choose a double coset $Wd_\lambda F_\lambda$ other than WF_λ. Suppose that d_λ ends in μ. If $W_j = Wd_\lambda$, then ${}^\lambda\overline{W}_j = d_\lambda = {}^\mu\overline{W}_j$, so that K contains $z_{j\lambda} z_{j\mu}^{-1}$, ($j \neq 1$, $\lambda \neq \mu$). Conversely, let $z_{j\lambda} z_{j\mu}^{-1} \in K$ where $j \neq 1$ and $\lambda \neq \mu$. Then ${}^\lambda\overline{W}_j = {}^\mu\overline{W}_j = u$ say. Now $W_j \subseteq Wd_\lambda F_\lambda \cap Wd_\mu F_\mu$ for some d_λ, d_μ. Then $u \in d_\lambda F_\lambda \cap d_\mu F_\mu$, so that either $u = d_\lambda$ ends in μ or $u = d_\mu$ ends in λ. In this way one sees that there is a bijection between relators of the form $z_{j\lambda} z_{j\mu}^{-1}$ ($j \neq 1$, $\lambda \neq \mu$) and double cosets not of the form WF_λ. The number of relators is therefore $\sum_{\lambda \in \Lambda}(m_\lambda - 1)$. If $|\Lambda| = n$, the number of free generators $z_{j\lambda}$ of Z is $(m-1)(n-1)$. Each relator removes one $z_{j\lambda}$. Hence the rank of W_0 is

$$(m-1)(n-1) - \sum_{\lambda \in \Lambda} (m_\lambda - 1) = \sum_{\lambda \in \Lambda} (m - m_\lambda) + 1 - m. \qquad \square$$

Proof of the Subgroup Theorem (Concluded)

Let H be any subgroup of $G = \operatorname{Fr}_{\lambda \in \Lambda} G_\lambda$. Choose presentations $\varphi_\lambda : F_\lambda \to G_\lambda$ where F_λ is free, and let F be the free product $\operatorname{Fr}_{\lambda \in \Lambda} F_\lambda$. Then the φ_λ extend to a unique surjective homomorphism $\varphi: F \to G$. Let W be the preimage of H under φ and put $R = \operatorname{Ker} \varphi$.

Let a Kuroš system of transversals and double coset representatives for H be chosen. If $g_\lambda \in G_\lambda$, we choose an fix an element $f_\lambda \in F_\lambda$ such that $f_\lambda^\varphi = g_\lambda$. If $g = g_{\lambda_1} \cdots g_{\lambda_k}$ is the reduced form of g in G, write $f = f_{\lambda_1} \cdots f_{\lambda_k}$, which is the reduced form of f in F. Thus $f^\varphi = g$. In this way we obtain elements of F that map to the double coset representatives and transversal elements of H in G. It is easy to see that these elements of F form a Kuroš system of transversals for W in F.

Using this system of transversals, we obtain a set of relators for $\tau: \hat{F} \to W$ as in 6.3.8. Now $\tau\varphi: \hat{F} \to H$ is an epimorphism whose kernel is obviously the preimage of R under τ. Also R is the normal closure in F of $\bigcup_{\lambda \in \Lambda} \operatorname{Ker} \varphi_\lambda$ (by 6.2.7). Let r be a relator for φ_λ. Since $r \in R \leq W$ and $R \lhd F$, we have

$W_i r = W_i$ for all i. Hence by 6.3.4

$$(r^{W_i})^\tau = {}^\lambda W_i r({}^\lambda \overline{W}_i)^{-1} \in R.$$

This shows that the preimage of R under τ is the normal closure in $\hat{F}$ of all the r^{W_i} and of $K = \text{Ker}\,\tau$. Thus we obtain a set of relators for $\tau\varphi\colon \hat{F} \to H$ by adding to those for τ the elements r^{W_i}, where r is a relator for φ_λ.

Hence every defining relator of $\tau\varphi$ belongs to a free factor of $\hat{F}$. Consequently H is the free product of $H_0 = Z^{\tau\varphi}$ and the $(\hat{F}_{\lambda d})^{\tau\varphi} = (W \cap dF_\lambda d^{-1})^\varphi = H \cap d^\varphi G_\lambda (d^\varphi)^{-1}$ (by (10)). Since the relators in Z are the $z_{j\lambda} z_{j\mu}^{-1}$, the subgroup H_0 is isomorphic with $W_0 = Z^\tau$. Applying 6.3.9 we obtain the formula for the rank of H_0. □

The Subgroup Theorem has many applications. Here is an example.

6.3.10 (Baer–Levi†). *A group cannot be expressed in a nontrivial way as both a free product and a direct product.*

Proof. Let $G = A * B = C \times D$ where A, B, C, D are nontrivial groups. If $A \cap C \neq 1$, then $C_G(A \cap C) \leq A$ by 6.2.6; therefore $D \leq A$. Hence $C_G(D) \leq A$ by 6.2.6 again, which means that $C \leq A$ and $A = G$, a contradiction. Thus $A \cap C = 1$. For similar reasons $A \cap D$, $B \cap C$, and $B \cap D$ are all trivial. Since C and D are normal in G, they intersect conjugates of A and B trivially. Applying 6.3.1 we conclude that C and D are free groups. Now $A \simeq AC/C \leq G/C \simeq D$. Therefore A is free by the Nielsen–Schreier Theorem. Similarly B is free, so that $G = A * B$ is free. Let $1 \neq c \in C$ and $1 \neq d \in D$; then $\langle c, d\rangle$ is abelian. But $\langle c, d\rangle$ is also a free group, so it must be infinite cyclic; this is impossible in view of $\langle c\rangle \cap \langle d\rangle = 1$. □

The Grushko–Neumann Theorem

We mention without proof another very important theorem about free products, the Grushko–Neumann Theorem.

If F is a finitely generated free group and φ is a homomorphism from F onto a free product $G = \text{Fr}_{\lambda\in\Lambda} G_\lambda$, then F is a free product of groups F_λ, $\lambda \in \Lambda$, such that $F_\lambda^\varphi = G_\lambda$.

One of the most useful consequences of this theorem is the following. Let $G = G_1 * \cdots * G_n$ and let $d(G_i)$ be the minimum number of generators of the finitely generated group G_i. Then $d(G) = d(G_1) + \cdots + d(G_n)$ (see Exercise 6.3.11).

A geometrical approach to the Grushko–Neumann Theorem, as well as to the Kuroš Subgroup Theorem, can be found in b43].

† Friedrich Wilhelm Levi (1888–1966).

EXERCISES 6.3

1. Describe the structure of subgroups of PSL(2, $\mathbb{Z}$).
2. Which soluble groups can be embedded in a free product of cyclic groups?
3. A subgroup of a free product of abelian groups is also a free product of abelian groups.
4. A group is called *freely indecomposable* if it cannot be expressed as a free product of nontrivial groups. Let $G = \langle A, B \rangle$ where A and B are freely indecomposable and $A \cap B \neq 1$. Prove that G is freely indecomposable.
5. Let $G = \mathrm{Fr}_{\lambda \in \Lambda} G_\lambda = \mathrm{Fr}_{\mu \in M} H_\mu$ where the G_λ and H_μ are freely indecomposable. Prove that $|\Lambda| = |M|$ and that, with suitable relabeling, $G_\lambda \simeq H_\lambda$. If G_λ is not infinite cyclic, show that G_λ and H_λ are conjugate.
6. Prove that the following pairs of groups are not isomorphic;
   (a) $\langle x, y, z \mid x^2 = y^3 = z^4 = 1 \rangle$ and $\langle u, v, w \mid u^2 = v^3 = w^4 = 1, uv = vu \rangle$;
   (b) $\langle x, y, z \mid x^2 = y^3 = (xy)^2 = z^2 = 1 \rangle$ and $\langle u, v, w \mid u^2 = v^3 = w^2 = 1, uv = vu \rangle$;
   (c) $\langle x, y, z, t \mid xy = yx, zt = tz \rangle$ and $\langle s, u, v, w \mid su^2 = u^2 s, vw = wv \rangle$.
7. Every nontrivial direct product is freely indecomposable. Every nontrivial free product is directly indecomposable.
8. Prove 6.3.3(ii), that $(uv)^{W_i} = u^{W_i} v^{W_{iu}}$ if $u, v \in F_\lambda$.
9. Prove that the product rule (6.3.2) is not always valid. [*Hint*: Consider $(xy^{-1} \cdot y)^W$ where $x \in F_\lambda$, $y \in F_\mu$ and $\lambda \neq \mu$.]
10. Complete the proof of 6.3.7 by showing that $z_{i\lambda}^{\chi} \equiv z_{i\lambda} \bmod N$.
11. If $G = G_1 * G_2 * \cdots * G_n$ is a finitely generated group, prove that $d(G) = d(G_1) + d(G_2) + \cdots + d(G_n)$ by applying the Grushko–Neumann Theorem.
12. Prove that every finitely generated group can be expressed as a free product of finitely many freely indecomposable groups. Show also that this decomposition is unique up to order.
13. Let G be the group with the presentation $\langle x_1, \ldots, x_n \mid [x_1, x_2] = [x_2, x_3] = \cdots = [x_{n-1}, x_n] = 1 \rangle$. Prove that G is freely indecomposable. [*Hint*: Assume that $G = H * K$ where $H \neq G$ and $K \neq G$. Let $C = C_G(x_1)$ and apply 6.3.1 and 6.2.6 to show that $C = 1$.]

6.4. Generalized Free Products

Let there be given a nonempty set of groups $\{G_\lambda \mid \lambda \in \Lambda\}$, together with a group H which is isomorphic with a subgroup H_λ of G_λ by means of a monomorphism

$$\varphi_\lambda : H \to G_\lambda \qquad (\lambda \in \Lambda).$$

There is an exceedingly useful object known as the *free product of the G_λ's with the amalgamated subgroup H*. Roughly speaking this is the largest

group generated by the G_λ's in which the subgroups H_λ are identified by means of the φ_λ. Generically such groups are known as *generalized free products*.

The precise definition follows. Let there be given groups G_λ and monomorphism $\varphi_\lambda: H \to G_\lambda$ as before. Define F to be the free product $\mathrm{Fr}_{\lambda \in \Lambda} G_\lambda$ and let N be the normal closure in F of the subset

$$\{(h^{\varphi_\lambda})^{-1} h^{\varphi_\mu} | \lambda, \mu \in \Lambda, h \in H\}.$$

The *free product of the G_λ with amalgamated subgroup H* (with respect to the φ_λ) is defined to be the group

$$G = F/N.$$

The point here is that $h^{\varphi_\lambda} \equiv h^{\varphi_\mu} \bmod N$, so that all the subgroups $H^{\varphi_\lambda}N/N$ are equal in G. In general G will depend on the particular φ_λ chosen, not merely on the subgroups H_λ—see Exercise 6.4.9. Of course when $H = 1$, the generalized free product reduces to the free product.

The case which is most commonly encountered is when there are two groups G_1, G_2 with subgroups H_1, H_2 that are isomorphic via $\varphi: H_1 \to H_2$; this arises when $H = H_1$ and the monomorphisms in the definition are $\varphi_1 = 1$ and $\varphi_2 = \varphi$.

An Example

Let $A = \langle a \rangle$ and $B = \langle b \rangle$ be cyclic groups of orders 4 and 6 respectively. The free product $A * B$ has the presentation $\langle a, b | a^4 = 1 = b^6 \rangle$. Since a^2 and b^3 both have order 2, the subgroups $\langle a^2 \rangle$ and $\langle b^3 \rangle$ are isomorphic; we may therefore form the free product G with an amalgamation determined by the isomorphism $\langle a^2 \rangle \to \langle b^3 \rangle$. This amounts to identifying a^2 and b^3. Thus G has the presentation

$$\langle a, b | a^4 = 1, a^2 = b^3 \rangle.$$

Here we have not troubled to change the names of the generators.

The element $h = a^2 = b^3$ commutes with a and b, so it belongs to the center of G. Therefore every element of G can be written in the form

$$h^i a^{j_1} b^{k_1} a^{j_2} b^{k_2} \cdots a^{j_r} b^{k_r}, \qquad (r \geq 0),$$

where i and $j_s = 0$ or 1 and $k_s = 0$, 1, or 2. It is reasonable to ask whether the above expression is unique, at least if identity elements are deleted and consecutive terms lie in different factors.

One way to see that this is true is to map G homomorphically onto the group $L = \langle u \rangle * \langle v \rangle$ where u and v have orders 2 and 3 respectively. This can be done by means of the assignments $a \mapsto u$ and $b \mapsto v$ using von Dyck's Theorem (2.2.1). If an element of G had two expressions of the above type, some element of L would have two normal forms, which is known to be impossible. Therefore every element of G has a unique expression.

Guided by this example we proceed to the general case.

Normal Form in Generalized Free Products

Let G be the free product of groups G_λ, $\lambda \in \Lambda$, with a subgroup amalgamated according to monomorphisms $\varphi_\lambda: H \to G_\lambda$: write H_λ for $\operatorname{Im} \varphi_\lambda$. If $F = \operatorname{Fr}_{\lambda \in \Lambda} G_\lambda$ and N is the normal closure in F of the set of all $(h^{\varphi_\lambda})^{-1} h^{\varphi_\mu}$, $h \in H$, $\lambda, \mu \in \Lambda$, then $G = F/N$.

For each $\lambda \in \Lambda$ we choose and fix a right transversal to $H_\lambda = H^{\varphi_\lambda}$ in G_λ, writing $\bar{g}$ for the representative of the coset $H_\lambda g$; of course we choose $\bar{1} = 1$. Consider an element f of F written in the normal form for the free product, $f = u_1 u_2 \cdots u_r$ where $u_i \in G_{\lambda_i}$. For convenience put $G_i = G_{\lambda_i}$ and $\varphi_i = \varphi_{\lambda_i}$. We shall define certain elements g_i in G_{λ_i}, starting with $g_r = u_r$. Write $g_r = h_r^{\varphi_r} \bar{g}_r$ where $h_r \in H$. Since $h_r^{\varphi_r} \equiv h_r^{\varphi_{r-1}} \bmod N$, we have $g_r \equiv h_r^{\varphi_{r-1}} \bar{g}_r \bmod N$. On substituting for $g_r = u_r$ in f, we obtain

$$f \equiv u_1 \cdots u_{r-2} g_{r-1} \bar{g}_r \mod N$$

where $g_{r-1} = u_{r-1} h_r^{\varphi_{r-1}} \in G_{r-1}$. Again $g_{r-1} \equiv h_{r-1}^{\varphi_{r-2}} \bar{g}_{r-1} \bmod N$ for some h_{r-1} in H. Hence

$$f \equiv u_1 \cdots u_{r-3} g_{r-2} \bar{g}_{r-1} \bar{g}_r \mod N$$

where $g_{r-2} = u_{r-2} h_{r-1}^{\varphi_{r-2}} \in G_{r-2}$.

After $r - 2$ further applications of this technique we obtain an expression

$$f \equiv h^{\varphi_1} \bar{g}_1 \cdots \bar{g}_r \mod N \tag{11}$$

where $h \in H$. Here $h^{\varphi_1} \equiv h^{\varphi_i} \bmod N$ for all i. This indicates what type of normal form is to be expected in a generalized free product.

Definition. Let $f \in F = \operatorname{Fr}_{\lambda \in \Lambda} G_\lambda$. A *normal form* of f with respect to the monomorphisms $\varphi_\lambda: H \to G_\lambda$ and the chosen transversals is a formal expression

$$h\bar{g}_1 \bar{g}_2 \cdots \bar{g}_r, \qquad (r \geq 0),$$

with the property $f \equiv h^{\varphi_{\lambda_1}} \bar{g}_1 \cdots \bar{g}_r \bmod N$: here $h \in H$, $g_i \in G_{\lambda_i}$ and we stipulate that $\bar{g}_i \neq 1$ and $\lambda_i \neq \lambda_{i+1}$.

The foregoing considerations demonstrate that each element of F has a normal form obtainable by the canonical process that led to (11). But the really important point remains to be settled, the uniqueness of the normal form.

6.4.1. *Each element of $F = \operatorname{Fr}_{\lambda \in \Lambda} G_\lambda$ has a unique normal form with respect to the monomorphisms $\varphi_\lambda: H \to G_\lambda$ and the fixed transversals to $H_\lambda = \operatorname{Im} \varphi_\lambda$ in G_λ.*

Proof. Since a direct proof of uniqueness would be technically very complicated, we adopt a different approach.

Let M denote the set of all normal forms of elements of F. Associate with each x in G_λ a permutation x^* of M defined in the following manner: $(h\bar{g}_1 \cdots \bar{g}_r)x^*$ is the normal form of the element $h^{\varphi_{\lambda_1}}\bar{g}_1 \cdots \bar{g}_r x$ which results on applying the canonical procedure described above. In what follows we write φ_i for φ_{λ_i}.

We claim that

$$(xy)^* = x^*y^*$$

for all x and y in G_λ. This is quite straightforward to prove but it does require some case distinctions.

Consider the normal form $h\bar{g}_1 \cdots \bar{g}_n$; assume that $\lambda_n \neq \lambda$, so $\bar{g}_n \notin G_\lambda$. Applying our procedure for constructing a normal form to $h^{\varphi_1}\bar{g}_1 \cdots \bar{g}_n x$, we obtain

$$(h\bar{g}_1 \cdots \bar{g}_n)x^* = (hh_1)\overline{g_1 h_2^{\varphi_1}} \cdots \overline{g_n h_{n+1}^{\varphi_n}}\,\bar{x} \tag{12}$$

where $h_i \in H$, $x = h_{n+1}^{\varphi_\lambda}\bar{x}$, and $\bar{g}_i h_{i+1}^{\varphi_i} = h_i^{\varphi_i}\overline{g_i h_{i+1}^{\varphi_i}}$, except that $\bar{x}$ must be deleted if $x \in H_\lambda$. Now apply y^*: we obtain elements k_i of H such that

$$(h\bar{g}_1 \cdots \bar{g}_n)x^*y^* = (hh_1k_1)\overline{g_1(h_2k_2)^{\varphi_1}} \cdots \overline{g_n(h_{n+1}k_{n+1})^{\varphi_n}}\,\overline{xy} \tag{13}$$

where $\bar{x}y = k_{n+1}^{\varphi_\lambda}\overline{xy}$ and $\overline{g_i h_{i+1}^{\varphi_i}}k_{i+1}^{\varphi_i} = k_i^{\varphi_i}\overline{g_i(h_{i+1}k_{i+1})^{\varphi_i}}$: here $\overline{xy}$ is to be deleted if $xy \in H_\lambda$. Replacing x by xy in (12), we obtain elements l_i of H such that

$$(h\bar{g}_1 \cdots \bar{g}_n)(xy)^* = (hl_1)\overline{g_1 l_2^{\varphi_1}} \cdots \overline{g_n l_{n+1}^{\varphi_n}}\,\overline{xy}$$

where $xy = l_{n+1}^{\varphi_\lambda}\overline{xy}$ and $\bar{g}_i l_{i+1}^{\varphi_i} = l_i^{\varphi_i}\overline{g_i l_{i+1}^{\varphi_i}}$. From the equations supporting (12) and (13) we find that $xy = (h_{n+1}k_{n+1})^{\varphi_\lambda}\overline{xy}$, and also $\bar{g}_i(h_{i+1}k_{i+1})^{\varphi_i} = (h_ik_i)^{\varphi_i}\overline{g_i(h_{i+1}k_{i+1})^{\varphi_i}}$. Hence $l_i = h_ik_i$ and $(h\bar{g}_1 \cdots \bar{g}_n)(xy)^* = (h\bar{g}_1 \cdots \bar{g}_n)x^*y^*$, by induction on $n + 1 - i$. The case $\lambda_n = \lambda$ is handled in a similar fashion.

It follows that $x \mapsto x^*$ is a homomorphism θ_λ from G_λ to Sym M. Hence there is a homomorphism $\theta\colon F \to \text{Sym}\, M$ which induces θ_λ in G_λ. Since $(h^{\varphi_\lambda})^{-1}h^{\varphi_\mu} \in N$, the permutation of M that corresponds to this element is the identity. Thus θ maps all elements of N to the identity.

If $h\bar{g}_1 \cdots \bar{g}_n$ is a normal form of f, then by definition

$$f \equiv h^{\varphi_1}\bar{g}_1 \cdots \bar{g}_n \mod N.$$

Hence $f^\theta = h^{\varphi_1\theta}\bar{g}_1^* \cdots \bar{g}_n^*$, which maps the normal form 1 to $h\bar{g}_1 \cdots \bar{g}_n$. It follows that f cannot have two normal forms. □

It is now possible to elucidate the structure of generalized free products.

6.4.2. *Let G be the free product of the groups G_λ with a subgroup H amalgamated via monomorphisms $\varphi_\lambda\colon H \to G_\lambda$. Then there exist subgroups $\bar{H}$ and $\bar{G}_\lambda$ of G isomorphic with H and G_λ respectively such that $G = \langle \bar{G}_\lambda | \lambda \in \Lambda\rangle$. Moreover $\bar{H}$ is the intersection of $\bar{G}_\lambda$* and *$\langle \bar{G}_\mu | \mu \in \Lambda, \mu \neq \lambda\rangle$.*

Proof. Let $F = \text{Fr}_{\lambda \in \Lambda} G_\lambda$ and let N denote the normal closure of the set of all $(h^{\varphi_\lambda})^{-1}h^{\varphi_\mu}$ $(h \in H, \lambda, \mu \in \Lambda)$. Thus $G = F/N$. Put $\bar{H} = H^{\varphi_\lambda}N/N$, which is independent of λ, and $\bar{G}_\lambda = G_\lambda N/N$. Then $H^{\varphi_\lambda} \cap N = 1$ and $G_\lambda \cap N = 1$ by

uniqueness of the normal form. Hence $\bar{H} \simeq H$ and $\bar{G}_\lambda \simeq G_\lambda$. Also

$$G_\lambda N \cap \langle G_\mu N | \mu \in \Lambda, \mu \neq \lambda \rangle = HN$$

by uniqueness of normal form again. Finally the $\bar{G}_\lambda$ generate G because the G_λ generate F. □

In order to simplify the notation we shall identify the subgroups $\bar{G}_\lambda$ and G_λ, and likewise $\bar{H}$ and H. Thus the G_λ are actually subgroups of their generalized free product G, which they also generate: also $G_\lambda \cap G_\mu = H$ if $\lambda \neq \mu$. An element of G may now be identified with its unique normal form

$$g = h\bar{g}_1 \cdots \bar{g}_r \qquad (r \geq 0),$$

$h \in H$, $g_i \in G_{\lambda_i} \backslash H$, $\lambda_i \neq \lambda_{i+1}$. Bear in mind that this expression is dependent on the choice of transversal to H in G_λ.

Just as in free products, uniqueness of the normal form is useful in locating elements of finite order.

6.4.3. *Let G be a generalized free product of groups G_λ, $\lambda \in \Lambda$, in which H is amalgamated.*

(i) *If $g = h\bar{g}_1 \cdots \bar{g}_n$ is the normal form of g (with respect to some set of transversals) and g_1 and g_n belong to different factors G_{λ_1} and G_{λ_n}, then g has infinite order.*
(ii) *If there are at least two G_λ's not equal to H, then G has an element of infinite order.*
(iii) *An element of G which has finite order is conjugate to an element of some G_λ.*

Proof. (i) Let us examine the normal form of powers of g. For example, consider $g^2 = h\bar{g}_1 \cdots \bar{g}_{n-1}(\bar{g}_n h)\bar{g}_1 \cdots \bar{g}_n$. Using expressions such as $\bar{g}_n h = h'\bar{g}_n'$ ($h' \in H$, $1 \neq g_n' \in G_{\lambda_n}$), we can move the h to the left, obtaining a normal form with $2n$ factors $\bar{g}_i$ or $\bar{g}_i'$; thus $g^2 \neq 1$. Similarly $g^m \neq 1$ if $m > 2$.

(ii) This follows from (i).

(iii) Suppose that $g^m = 1$ but g is not conjugate to any element of G_λ. Write $g = h\bar{g}_1 \cdots \bar{g}_n$, the normal form, with $g_i \in G_{\lambda_i}$. Then $n > 1$; for otherwise $g \in G_{\lambda_1}$. It follows from (i) that $\lambda_1 = \lambda_n$ and $n > 2$. Now $g' = \bar{g}_n g \bar{g}_n^{-1}$ has the normal form $h'\bar{g}_1'\bar{g}_2 \cdots \bar{g}_{n-1}$ where $h' \in H$ and $g_1' \in G_{\lambda_1}$. We deduce from (i) that $n = 2$, a contradiction. □

6.4.4. *A generalized free product of torsion-free groups is torsion-free.*

This is an immediate corollary of 6.4.3.

Embedding Theorems

One of the great uses of generalized free products is to embed a given group in a group with prescribed properties. In this subject the following theorem is basic.

6.4.5 (G. Higman, B.H. Neumann, H. Neumann†). *Let H and K be subgroups of a group G and let $\theta: H \to K$ be an isomorphism. Then G can be embedded in a group G^* such that θ is induced by an inner automorphism of G^*. What is more, if G is torsion-free, then so is G^*.*

Proof. Let $\langle u \rangle$ and $\langle v \rangle$ be infinite cyclic groups. Form the free products $X = G * \langle u \rangle$ and $Y = G * \langle v \rangle$. Now let $L = \langle G, H^u \rangle$ and $M = \langle G, K^v \rangle$. Then $L = G * H^u$ since there can be no nontrivial relation of the form $g_1 h_1^u g_2 h_2^u \cdots g_n h_n^u = 1$ with $g_i \in G$ and $h_i \in H$. Similarly $M = G * K^v$. Consequently there is a homomorphism $\varphi: L \to M$ such that $g^\varphi = g$ and $(h^u)^\varphi = (h^\theta)^v$, $(g \in G, h \in H)$. Clearly φ is an isomorphism.

Consider the generalized free product G^* of X and Y in which L and M are amalgamated by means of $\varphi: L \to M$. Thus $x^\varphi = x$ for x in L, and G is a subgroup of G^*. If $h \in H$, then $h^u = (h^u)^\varphi = (h^\theta)^v$, so that $h^\theta = h^{uv^{-1}}$ and θ is induced by conjugation by the element uv^{-1} of G^*. Notice that if G is torsion-free, so are X, Y, and G^* by 6.4.4. □

Write t for the element uv^{-1} of G^* that induces θ; then t will have infinite order by 6.4.3. The group $\langle t, G \rangle$ is called an HNN-*extension* of G (after Higman, Neumann, and Neumann). It may be thought of as the group generated by G and t subject to the relations $x^t = x^\theta$, $(x \in H)$.

HNN-extensions play an important part in modern combinatorial group theory (see [b43] for a detailed account).

The following embedding theorems illustrate the power of 6.4.5.

6.4.6 (Higman, Neumann, and Neumann). *A torsion-free group G can be embedded in a group U in which all nontrivial elements are conjugate. In particular U is torsion-free and simple.*

Proof. As a first step we embed G in a group G^* such that all nontrivial elements of G are conjugate in G^*. To achieve this, well-order the nontrivial elements of G, say as $\{g_\alpha | 0 \leq \alpha < \gamma\}$ for some ordinal γ. A chain of torsion-free groups $\{G_\alpha | 1 \leq \alpha < \gamma\}$ such that $G \leq G_\alpha$ and all the g_β with $\beta < \alpha$ are conjugate in G_α will be constructed. Let $G_1 = G$; suppose that G_β has been suitably constructed for all $\beta < \alpha$. If α is a limit ordinal, simply define G_α to be the union of all the G_β with $\beta < \alpha$. Suppose that α is not a limit ordinal, so that $G_{\alpha-1}$ has already been constructed. Now $\langle g_0 \rangle$ and $\langle g_{\alpha-1} \rangle$ are isomorphic subgroups of $G_{\alpha-1}$ since both are infinite cyclic. Applying 6.4.5 we embed $G_{\alpha-1}$ in a torsion-free group G_α in such a way that g_0 and $g_{\alpha-1}$ are conjugate in G_α. All the g_β, $0 \leq \beta < \alpha$, are now conjugate in G_α. Thus our chain has been constructed. Denote the union of the G_α, $1 \leq \alpha < \gamma$, by G^*. All nontrivial elements of G are conjugate in G^*.

† Hanna Neumann (1914–1971).

The proof is now easy. Define $G(0) = G$ and $G(i + 1) = (G(i))^*$. This defines recursively a countable chain of groups $G = G(0) \leq G(1) \leq \cdots$. Let U be the union of this chain. Any two nontrivial elements of U belong to some $G(i)$, so they are conjugate in $G(i + 1)$ and hence in G. □

On the basis of 6.4.6 we can assert that there exist groups of arbitrary infinite cardinality with just two conjugacy classes (cf. Exercise 1.6.8).

To conclude this chapter we shall prove what is probably the most famous of all embedding theorems.

6.4.7 (Higman, Neumann, and Neumann). *Every countable group can be embedded in a group which is generated by two elements of infinite order.*

Proof. Let $G = \{1 = g_0, g_1, g_2 \cdots\}$ be any countable group and let F be the free group on a two-element set $\{a, b\}$. We consider two subgroups of the free product $H = G * F$,

$$A = \langle a, a^b, a^{b^2}, \ldots \rangle \qquad \text{and} \qquad B = \langle bg_0, b^a g_1, b^{a^2} g_2, \ldots \rangle.$$

It is easy to see that a nontrivial reduced word in $a, a^b, a^{b^2}, \ldots$ cannot equal 1. Hence A is freely generated by $a, a^b, a^{b2}, \ldots$; for the same reason B is freely generated by $bg_0, b^a g_1, b^{a^2} g_2, \ldots$. Hence there is an isomorphism $\varphi: A \to B$ in which a^{b^i} is mapped to $b^{a^i} g_i$.

By 6.4.5 we can find an HNN-extension $K = \langle H, t \rangle$ such that $(a^{b^i})^t = b^{a^i} g_i$. The subgroup $\langle a, t \rangle$ contains $a^t = b$ and therefore $(a^{b^i})^t = b^{a^i} g_i$. Consequently $\langle a, t \rangle$ contains each g_i, and therefore equals K. Of course G is a subgroup of K.

It is obvious that a has infinite order. By a remark following 6.4.5 the order of t is also infinite. □

Exercises 6.4

1. Identify each of the following groups as a generalized free product, describing the factors and the amalgamated subgroups:
   (a) $\langle x, y \mid x^3 = y^3, y^6 = 1 \rangle$; and
   (b) $\langle x, y \mid x^{30} = 1 = y^{70}, x^3 = y^5 \rangle$.
2. Express $SL(2, \mathbb{Z})$ as a generalized free product.
3. Write in normal form the elements xyx^3y^2 and $y^5x^2yx^3y^3x$ of the group $\langle x, y \mid x^4 = 1 = y^6, x^2 = y^3 \rangle$.
4. Show that the *braid group on three strings* $G = \langle x, y \mid xyx = yxy \rangle$ is a generalized free product of two infinite cyclic groups. Deduce that G is torsion-free. [*Hint*: Let $u = xy$ and $v = xyx$.]
5. Find a mapping property which characterizes generalized free products.
6. Complete the proof of uniqueness of the normal form (6.4.1, case $\lambda_n = \lambda$).

7. Let G be generated by subgroups G_λ, $\lambda \in \Lambda$, and let $H \leq G_\lambda$ for all λ. Assume that there exist transversals to H in the G_λ such that each element of G admits a unique expression of the form $h\bar{g}_1 \cdots \bar{g}_n$ where $h \in H$, $g_i \in G_{\lambda_i} \backslash H$, $\lambda_i \neq \lambda_{i+1}$, and $\bar{g}_i$ is the coset representative of Hg_i in G_{λ_i}. Prove that G is a free product of the G_λ's with H amalgamated.

8. (a) Let G be a generalized free product of groups G_λ, $\lambda \in \Lambda$, with a proper amalgamated subgroup. Prove that the center of G equals $\bigcap_{\lambda \in \Lambda} \zeta(G_\lambda)$.
   (b) Locate the center of the group
$$\langle x, y, z, t \mid xy = yx, x^6 = z^3, x^4 = t^5 \rangle.$$

9. Show that the generalized free product depends on the amalgamating monomorphisms as follows. Let $G_i = \langle a_i, b_i \mid a_i^4 = 1 = b_i^2, b_i^{-1}a_ib_i = a_i^{-1} \rangle$, $i = 1, 2$, be two dihedral groups of order 8. Let H_i be an elementary abelian subgroup of G_i with order 4. Find two isomorphisms between H_1 and H_2 that lead to two non-isomorphic generalized products of G_1 and G_2 with H_1 and H_2 amalgamated.

10. Let $G = \langle x, y \mid x^2 = y^2 \rangle$. Prove that G is an extension of its center by an infinite dihedral group. Show that G is supersoluble and G' is cyclic.

11. A group is said to be *radicable* if every element is an nth power for all positive integers n. Using generalized free products, prove that every group can be embedded in a radicable group. (*Note*: For additive groups the term *divisible* is used instead of radicable.)

12. There exists a 2-generator group containing an isomorphic copy of every countable abelian group.

13. Prove that any group G can be embedded in a group G^* in which all elements of the same order are conjugate. Also if G is countable, then G^* can be assumed to be countable.

14. Prove that any countable group G can be embedded in a countable radicable simple group. [*Hint*: Embed G in group G_1 which contains elements of all possible orders and then embed G_1 in $G_2 = G_1 * \langle x \rangle$ where $|x| = \infty$. Now embed G_2 in a group G_3 with two generators of infinite order. Finally embed G_3 in a group G_4 in which all elements of equal order are conjugate.]

15. Exhibit G. Higman's group (see Exercise 3.2.9)
$$G = \langle b_1, b_2, b_3, b_4 \mid b_1^{b_4} = b_1^2, b_2^{b_1} = b_2^2, b_3^{b_2} = b_3^2, b_4^{b_3} = b_4^2 \rangle$$
as a generalized free product of torsion-free groups. Deduce that G is nontrivial and torsion-free. [*Hint*: Let $H_i = \langle a_i, b_i \mid b_i^{a_i} = b_i^2 \rangle$, $i = 1, 2, 3, 4$. Let K_{12} and K_{34} be the generalized free products of H_1 and H_2 and of H_3 and H_4 in which $b_1 = a_2$ and $b_3 = a_4$ respectively. Show that G is a generalized free product of K_{12} and K_{34}.]

CHAPTER 7

Finite Permutation Groups

The theory of finite permutation groups is the oldest branch of group theory, many parts of it having been developed in the nineteenth century. However, despite its antiquity, the subject continues to be an active field of investigation.

If G is a permutation group on a set X, it will be understood throughout this chapter that G and X are finite. Frequently it is convenient to take X to be the set $\{1, 2, \ldots, n\}$, so that $G \leq \text{Sym}\, X = S_n$. There is no real loss of generality here since we are only interested in permutation groups up to similarity.

If Y is a subset of X, the (pointwise) stabilizer $\text{St}_G(Y)$ of Y in G is often written simply

$$G_Y$$

in permutation group theory. We shall use this notation when it is not misleading. The elementary properties of permutation groups were developed in 1.6.

7.1. Multiple Transitivity

Suppose that G is a permutation group on a set X containing n elements. If $1 \leq k \leq n$, we shall write

$$X^{[k]}$$

for the set of all ordered k-tuples $(a_1, a_2, \ldots, a_k)$ consisting of *distinct* elements a_i of X. The group G acts in a very natural way on $X^{[k]}$, namely,

componentwise. Thus, if $\pi \in G$,

$$(a_1, \ldots, a_k)\pi = (a_1\pi, \ldots, a_k\pi) \tag{1}$$

and we have a permutation representation of G on $X^{[k]}$.

If G acts transitively on $X^{[k]}$, then G is said to be *k-transitive* as a permutation group on X. Thus 1-transitivity is simply transitivity, and, in fact, the strength of the property "k-transitive" increases with k. Suppose that G acts on X without actually being a group of permutations of X; then we shall say that G is *k-transitive on X* if G acts transitively on $X^{[k]}$ by means of the rule (1).

The following result is fundamental and is the basis of many induction arguments.

7.1.1. *Let G be a transitive permutation group on a set X. Suppose that $k > 1$ and a is a fixed element of X. Then G is k-transitive if and only if G_a is $(k-1)$-transitive on $X \backslash \{a\}$.*

Proof. Suppose first that G is k-transitive on X and let $(a_1, \ldots, a_{k-1})$ and $(a_1', \ldots, a_{k-1}')$ belong to $Y^{[k-1]}$ where $Y = X \backslash \{a\}$. Then $a_i \neq a \neq a_i'$ and by k-transitivity there is a permutation π in G mapping $(a_1, \ldots, a_{k-1}, a)$ to $(a_1', \ldots, a_{k-1}', a)$; now π fixes a and maps $(a_1, \ldots, a_{k-1})$ to $(a_1', \ldots, a_{k-1}')$, which shows that G_a acts $(k-1)$-transitively on Y.

Conversely suppose that G_a is $(k-1)$-transitive on Y. Let $(a_1, \ldots, a_k)$ and $(\bar{a}_1, \ldots, \bar{a}_k)$ belong to $X^{[k]}$. Since G is transitive on X, we can find π and $\bar{\pi}$ in G such that $a_1\pi = a$ and $\bar{a}_1 = a\bar{\pi}$. Moreover there exists a σ in G_σ mapping $(a_2\pi, \ldots, a_k\pi)$ to $(\bar{a}_2\bar{\pi}^{-1}, \ldots, \bar{a}_k\bar{\pi}^{-1})$ by $(k-1)$-transitivity of G_a. Thus we have $a_i\pi\sigma = \bar{a}_i\bar{\pi}^{-1}$ or $a_i\pi\sigma\bar{\pi} = \bar{a}_i$ for $i = 2, \ldots, k$. Also $a_1\pi\sigma\bar{\pi} = a\sigma\bar{\pi} = a\bar{\pi} = \bar{a}_1$ since $\sigma \in G_a$. Hence the element $\pi\sigma\bar{\pi}$ of G maps $(a_1, \ldots, a_k)$ to $(\bar{a}_1, \ldots, \bar{a}_k)$ and G is k-transitive on X. □

Notice the immediate consequence: *$(k+1)$-transitivity implies k-transitivity.*

If X has n elements, the number of elements in $X^{[k]}$ equals

$$n(n-1)\cdots(n-k+1),$$

the number of permutations of n objects taken k at a time. Using 1.6.1 we deduce at once the following important result.

7.1.2. *If G is a k-transitive permutation group of degree n, the order of G is divisible by $n(n-1)\cdots(n-k+1)$.*

Sharply k-Transitive Permutation Groups

Let G be a permutation group on a set X. If G acts regularly on $X^{[k]}$, then G is said to be *sharply k-transitive* on X. What this means is that, given two

k-tuples in $X^{[k]}$, there exists a *unique* permutation in G mapping one k-tuple to the other. Clearly sharp 1-transitivity is the same as regularity. By 1.6.1 we have at once

7.1.3. *A k-transitive permutation group G with degree n is sharply k-transitive if and only if the order of G equals $n(n-1)\cdots(n-k+1)$.*

The easiest examples of multiply transitive permutation groups are the symmetric and alternating groups.

7.1.4.

(i) *The symmetric group S_n is sharply n-transitive.*
(ii) *If $n > 2$, the alternating group A_n is sharply $(n-2)$-transitive.*
(iii) *Up to similarity S_n and A_n are the only $(n-2)$-transitive groups of degree n and S_n is the only $(n-1)$-transitive group of degree n.*

Proof. (i) This is obvious.

(ii) In the first place it is easy to see that A_n is transitive. Since A_3 is generated by $(1, 2, 3)$, it is regular and hence sharply 1-transitive: thus the statement is true when $n = 3$. Let $n > 3$ and define H to be the stabilizer of n in A_n. Then H acts on the set $\{1, 2, \dots, n-1\}$ to produce all even permutations. By induction H is $(n-3)$-transitive on $\{1, 2, \dots, n-1\}$, so A_n is $(n-2)$-transitive by 7.1.1. Since $|A_n| = \frac{1}{2}(n!) = n(n-1)\cdots 3$, we see from 7.1.3 that this is sharp $(n-2)$-transitivity.

(iii) Suppose that $G \leq S_n$. If G is $(n-2)$-transitive, then $n(n-1)\cdots 3 = \frac{1}{2}(n!)$ divides $|G|$ and $|S_n : G| = 1$ or 2. Hence $G \lhd S_n$, which implies that $G = A_n$ or S_n (by 3.2.3 and a direct argument when $n = 4$). Of course if G is $(n-1)$-transitive, then $G = S_n$. □

Examples of Sharply 2- and 3-Transitive Permutation Groups

We shall now discuss certain important types of sharply 2-transitive and 3-transitive permutation groups that are not of alternating or symmetric type.

Let F be a Galois field $GF(q)$ where $q = p^m$ and p is prime. We adjoin to F the symbol ∞: it may be helpful for the reader to think of the resulting set

$$X = F \cup \{\infty\}$$

as the projective line consisting of $q + 1$ points. Define

$$L(q)$$

to be the set of all functions $\alpha: X \to X$ of the form

$$x\alpha = \frac{ax + b}{cx + d}, \tag{2}$$

where a, b, c, d belong to F and $ad - bc \neq 0$. (Such a function is called a *linear fractional transformation.*) Here it is understood that the symbol ∞ is subject to such formal arithmetic rules as $x + \infty = \infty$, $\infty/\infty = 1$, etc.

It is easy to verify that $L(q)$ is a group with respect to functional composition: indeed $L(q)$ is isomorphic with the projective general linear group $\mathrm{PGL}(2, q)$—see Exercise 3.2.3. In the present context it is the natural action of $L(q)$ on X that concerns us. The stabilizer of ∞ in $L(q)$ is easily seen to be the subgroup

$$H(q)$$

of all functions $x \mapsto ax + b$, $(a \neq 0)$. Concerning the groups $H(q)$ and $L(q)$ we shall prove the following.

7.1.5. *The group $H(q)$ is sharply 2-transitive on $F = \mathrm{GF}(q)$ with degree q. The group $L(q)$ is sharply 3-transitive on $F \cup \{\infty\}$ with degree $q + 1$.*

Proof. In the first place $H(q)$ acts 2-transitively on F. For, given x, y, x', y' in F with $x \neq y$, $x' \neq y'$, we can solve the equations $x' = ax + b$ and $y' = ay + b$ for a, b in F with $a \neq 0$. Consequently there is a π in $H(q)$ mapping (x, y) to (x', y').

Next $L(q)$ is transitive on $X = F \cup \{\infty\}$ because $H(q)$ is transitive on F and the function $x \mapsto 1/x$ sends ∞ to 0. By 7.1.1 we conclude that $L(q)$ is 3-transitive on X. The order of $H(q)$ is clearly $q(q - 1)$, so $H(q)$ is sharply 2-transitive on F. Also $|L(q) : H(q)| = |X| = q + 1$; thus

$$|L(q)| = (q + 1)q(q - 1)$$

and the group $L(q)$ is sharply 3-transitive on X. □

It is clear that $H(q)$ is not regular, but a nontrivial element of $H(q)$ cannot fix more than one point of $\mathrm{GF}(q)$, by sharp 2-transitivity. A transitive permutation group with these properties is called a *Frobenius group*: more will be said of this important type of group in Chapters 8 and 10.

There is a second family of sharply 3-transitive permutation groups acting on the projective line. As before let $F = \mathrm{GF}(q)$ and $X = F \cup \{\infty\}$ where now $q = p^{2m}$ and $p > 2$. The mapping $\sigma: F \to F$ given by $x^\sigma = x^{p^m}$ is an automorphism of the field F with order 2 since $x^{p^{2m}} = x$. Extend σ to X by letting σ fix ∞.

Using this function $\sigma: X \to X$ we define

$$M(q)$$

to be the set of all functions $\alpha: X \to X$ which are of the form

$$x\alpha = \frac{ax + b}{cx + d},$$

where $ad - bc$ is a nonzero square in F, or of the form

$$x\alpha = \frac{ax^\sigma + b}{cx^\sigma + d},$$

where $ad - bc$ is not a square in F. A simple direct computation shows that $M(q)$ is a group with respect to functional composition. (*Note*: the product of two nonsquares is a square.)

Thus $M(q)$ is a permutation group on X. The stabilizer of ∞ in $M(q)$ is the subgroup $S(q)$ of all functions $x \mapsto ax + b$ with a a nonzero square in F and $x \mapsto ax^\sigma + b$ where a is not a square in F.

Let us establish the multiple transivity of $M(q)$ and $S(q)$.

7.1.6. *The group $S(q)$ is sharply 2-transitive on $F = GF(q)$ and the group $M(q)$ is sharply 3-transitive on $F \cup \{\infty\}$.*

Proof. Both the mappings $x \mapsto ax + b$ and $x \mapsto ax^\sigma + b$ send $(0, 1)$ to $(b, a + b)$ and one of them must belong to $S(q)$. Thus $S(q)$ is 2-transitive on F. We must calculate the order of $S(q)$. Now $x \mapsto x^2$ is an endomorphism of the multiplicative group of F whose kernel $\langle -1 \rangle$ has order 2. Hence, by the First Isomorphism Theorem, there are exactly $\frac{1}{2}(q - 1)$ nonzero squares in F. The number of nonsquares is therefore also $\frac{1}{2}(q - 1)$. It follows that the order of $S(q)$ is $2(\frac{1}{2}(q - 1) \cdot q) = q(q - 1)$. Hence $S(q)$ is sharply 2-transitive on F. Next $x \mapsto -1/x$ belongs to $M(q)$ and maps ∞ to 0, which shows that $M(q)$ is transitive on X. Applying 7.1.1 we conclude that $M(q)$ is 3-transitive on X. Also $|M(q) : S(q)| = q + 1$ by transitivity of $M(q)$; thus

$$|M(q)| = (q + 1)q(q - 1)$$

and $M(q)$ is sharply 3-transitive. □

It can be shown that the groups $L(q)$ and $M(q)$ are not isomorphic, so that we have two infinite families of sharply 3-transitive groups. The significance of these groups may be gauged from the theorem of Zassenhaus ([b50]) that every sharply 3-transitive permutation group is similar to either $L(q)$ or $M(q)$.

In 7.4 we shall construct sharply 4-transitive and 5-transitive groups which are not symmetric or alternating groups. However, if $k \geq 6$, no examples of k-transitive permutation groups which are not of symmetric or alternating type are known. Indeed according to the classification of finite simple groups no such examples exist (see [a22]).

Exercises 7.1

1. Using only the definition prove that a $(k + 1)$-transitive group is k-transitive.
2. A permutation group G of degree n is sharply k-transitive and sharply l-transitive where $k < l$ if and only if $k = n - 1$, $l = n$, and $G = S_n$.

3. If G is k-transitive but not $(k + 1)$-transitive, is it true that G is sharply k-transitive?

4. List all similarity types of transitive permutation group of degree ≤ 5. Give in each case the maximum degree of transitivity and say whether it is sharp or not.

5. Prove that a 3-transitive group G of degree 6 is similar to A_6, S_6, or $L(5)$. [*Hint*: Reduce to the case where $|G| = 120$ and G acts on $\mathrm{GF}(5) \cup \{\infty\}$ with $G_\infty = H(5)$. Show that G_∞ is maximal in G and consider the cycle type of elements in $G \backslash H(5)$.]

6. Let G be a permutation group on a set X. If $|X| > 1$, then G is called $\frac{1}{2}$-*transitive* if $|G| \neq 1$ and all G-orbits have the same length. (If $|X| = 1$, then G is considered as being $\frac{1}{2}$-transitive.) Also, if $1 \leq k < n$, the group G is said to be $(k + \frac{1}{2})$-*transitive* if G is transitive and G_a is $(k - \frac{1}{2})$-*transitive* for some (and hence all) a in X.
   (a) Prove that $(k + \frac{1}{2})$-transitivity implies k-transitivity and k-transitivity implies $(k - \frac{1}{2})$-transitivity.
   (b) If G is transitive and $1 \neq N \lhd G$, prove that N is $\frac{1}{2}$-transitive.

7. Let G be a permutation group on a set X. If H is a transitive subgroup of G, then $G = G_a H$ for all $a \in X$. Deduce that Frat G is never transitive if $|G| > 1$.

8. Let $F = \mathrm{GF}(q)$ where $q = p^m$ and p is prime. A *semilinear transformation* of F is a mapping of the form $x \mapsto ax^\sigma + b$ where $a, b \in F$, $a \neq 0$, and σ is a field automorphism of F.
   (a) Show that $\Gamma(q)$, the set of all semilinear transformations of F, is a soluble group of order $mq(q - 1)$.
   (b) Prove that $\Gamma(q)$ is 2-transitive.
   (c) Prove that $\Gamma(q)$ is 3-transitive if and only if $q = 3$ or 4, when $\Gamma(q)$ is similar to S_3 or S_4 respectively.
   (d) Prove that $\Gamma(q)$ is $\frac{5}{2}$-transitive if and only if $q = 3$ or $q = 2^m$ where m is prime. [*Hint*: $G = \Gamma(q)$ is $\frac{5}{2}$-transitive if and only if $G_{\{0,1\}}$ is $\frac{1}{2}$-transitive on $F \backslash \{0, 1\}$, and $G_{\{0,1\}}$ is the group of field automorphisms.]

7.2. Primitive Permutation Groups

Let G be a transitive permutation group on a set X. A proper subset Y of X with at least two elements is called a *domain of imprimitivity* of G if, for each permutation π in G, either $Y = Y\pi$ or $Y \cap Y\pi = \varnothing$. The group G is then said to be *imprimitive*. On the other hand, should G possess no domain of imprimitivity, it is called *primitive*. For example, one quickly verifies that S_n is primitive for all $n \geq 1$.

The essential point about an imprimitive group is that the permuted set has a partition the members of which are permuted under the action of the group. More precisely the following holds.

7.2.1. *Let G be a transitive permutation group on X. Let Y be a domain of imprimitivity of G and denote by H the subgroup of all π in G such that $Y\pi = Y$. Choose a right transversal T to H in G.*

(i) *The subsets* $Y\tau$, $\tau \in T$, *form a partition of* X.
(ii) *In the natural action* G *permutes the subsets* $Y\tau$ *in the same way as it does the right cosets of* H, *namely by right multiplication.*
(iii) $|X| = |Y| \cdot |T|$, *so that* $|Y|$ *divides* $|X|$.

Proof. Let $a \in X$ and $b \in Y$. On account of the transitivity of G there is a π in G such that $a = b\pi$. Writing $\pi = \sigma\tau$ with σ in H and τ in T, we have $a = (b\sigma)\tau \in Y\tau$, so that X is certainly the union of the $Y\tau$, $\tau \in T$. Next, if $Y\tau \cap Y\tau' \neq \varnothing$, then $Y \cap Y\tau'\tau^{-1} \neq \varnothing$. Hence $Y = Y\tau'\tau^{-1}$ and $\tau'\tau^{-1} \in H$ because Y is a domain of imprimitivity. Since τ and τ' are members of a transversal, $\tau = \tau'$. Thus (i) has been established. (iii) follows at once because $|Y\tau| = |Y|$.

If $\tau \in T$ and $\pi \in G$, then $H\tau\pi = H\tau'$ where $H\tau \mapsto H\tau'$ is a permutation of the set of right cosets of H. Thus $(Y\tau)\pi = Y\tau'$, which proves (ii). □

On the basis of this result we can state

7.2.2. *A transitive permutation group of prime degree is primitive.*

The next result is a valuable criterion for primitivity.

7.2.3. *Let* G *be a transitive permutation group on a set* X *and let* $a \in X$. *Then* G *is primitive if and only if* G_a *is a maximal subgroup of* G.

Proof. Assume that G_a is not maximal, so that there is an H satisfying $G_a < H < G$. Define Y to consist of all $a\sigma$ where $\sigma \in H$. Then $|Y| \geq 2$ since $H > G_a$. Suppose that $Y = X$. Then for any π in G one can write $a\pi = a\sigma$ for some σ in H; thus $\pi\sigma^{-1} \in G_a$, which gives $\pi \in H$ and $G = H$. Finally, if $Y \cap Y\pi \neq \varnothing$ and $a\sigma_1 = a\sigma_2\pi$ with σ_i in H, then $\sigma_2\pi\sigma_1^{-1} \in G_a < H$ and $\pi \in H$, which implies that $Y = Y\pi$. Consequently Y is a system of imprimitivity and G is imprimitive.

Conversely suppose that Y is a system of imprimitivity of G: notice that we may assume a to be in Y in view of the transitivity of G. Define $H = \{\pi \in G \mid Y\pi = Y\}$; then $H \leq G$. Now H acts transitively on Y; for if b, $c \in Y$, there is a π in G such that $b\pi = c$; but then $c \in Y \cap Y\pi$, so $Y = Y\pi$ and $\pi \in H$. Hence $|Y| = |H : H_a|$. If $\pi \in G_a$, then $a = a\pi \in Y \cap Y\pi$, whence $Y = Y\pi$ and $\pi \in H$; this shows that $G_a \leq H$ and $G_a = H_a$. Finally we have $|X| = |G : G_a|$ and $|Y| = |H : H_a| = |H : G_a|$, so that $G_a < H < G$ and G_a is not maximal in G. □

The 2-transitive groups constitute a frequently encountered source of primitive groups.

7.2.4. *Every 2-transitive permutation group is primitive.*

Proof. Let G be a 2-transitive permutation group on a set X and suppose that Y is a domain of imprimitivity of G. Then two distinct elements a and b

can be found in Y and also an element c in $X \backslash Y$. By 2-transitivity there is a π in G such that $(a, b)\pi = (a, c)$. Then $a \in Y \cap Y\pi$, whence $Y = Y\pi$; but this implies that $c = b\pi \in Y$, a contradiction. □

Soluble Primitive Permutation Groups

Before discussing groups of the above type we take note of an important property of normal subgroups of primitive groups.

7.2.5. *If N is a nontrivial normal subgroup of a primitive permutation group G on X, then N is transitive on X.*

Proof. Let Y be an N-orbit of X and let $a \in Y$. Thus $Y = \{a\sigma | \sigma \in N\}$. If $\pi \in G$ and $\sigma \in N$, then $(a\sigma)\pi = (a\pi)\sigma^\pi$ and $\sigma^\pi \in N$; thus we recognize $Y\pi$ to be the N-orbit containing $a\pi$. Hence either $Y = Y\pi$ or $Y \cap Y\pi = \emptyset$. But Y cannot be a domain of imprimitivity since G is primitive. Hence either $Y = X$, and N is transitive, or every N-orbit has just one element and $N = 1$. □

7.2.6. *Let G be a primitive permutation group on a set X and suppose that G has a minimal normal subgroup N which is abelian. Then N is an elementary abelian p-group of order p^m for some prime p. Also $N = C_G(N)$ and N is the unique minimal normal subgroup of G. Moreover $H = G_aN$ and $G_a \cap N = 1$ for any a in X. The degree of G is p^m.*

Proof. By 7.2.5 the abelian subgroup N is transitive and by 1.6.3 it is regular. Hence $|X| = |N|$; moreover $|N| = p^m$ for some prime p since N must be elementary abelian, being abelian and minimal normal in G. Regularity also implies that $G_a \cap N = 1$ for any a in X. Now G_a is maximal in G by 7.2.3, so $G = G_aN$. Hence $C_G(N) = C_{G_a}(N)N$. If $\pi \in C_{G_a}(N)$ and $\sigma \in N$, then $a\sigma\pi = a\pi\sigma = a\sigma$. Since N is transitive, it follows that $\pi = 1$; therefore $C_{G_a}(N) = 1$ and $C_G(N) = N$. Finally, if $\bar{N}$ is a minimal normal subgroup of G other than N, then $N \cap \bar{N} = 1$ and $[N, \bar{N}] = 1$; by our previous conclusion $\bar{N} \leq N$ and $\bar{N} = 1$, which is impossible. □

This result applies in particular to soluble primitive permutation groups because a minimal normal subgroup of soluble group is abelian. Thus a soluble primitive permutation group must have prime-power degree.

The Affine Group

The groups of 7.2.6 may be realized as subgroups of the affine group of a vector space. Let V be a vector space over a field F and regard the group

$G = \mathrm{GL}(V)$ of all linear transformations of V as a permutation group on V. Another group of permutations of V is relevant here, the group of translations of V. If $v \in V$, the associated *translation* v^* is the permutation of V mapping x to $x + v$; this is a permutation since $(-v)^*$ is obviously the inverse of v^*. The mapping $v \mapsto v^*$ is a monomorphism from the additive group of V into Sym V, the image V^* being the *translation group* of V.

The *affine group* of V is now defined to be the subgroup of Sym V generated by G and V^*:

$$A = \mathrm{Aff}(V) = \langle G, V^* \rangle.$$

Let us elucidate the structure of this group. If $x, v \in V$ and $\gamma \in G$, then $\gamma^{-1}v^*\gamma$ maps x to $(x\gamma^{-1} + v)\gamma = x + v\gamma$; therefore

$$\gamma^{-1}v^*\gamma = (v\gamma)^*. \tag{3}$$

This equation implies that $V^* \lhd A$ and $A = GV^*$. Clearly the stabilizer in A of the zero vector is G since no nontrivial element of V^* fixes this vector; thus $G \cap V^* = 1$. In summary, A is the semidirect product of V^* by G where the action of G on V^* is described by (3).

7.2.7. *The group G of* 7.2.6 *is similar to a subgroup of* Aff(V) *containing the translation group where V is a vector space with dimension m over* GF(p).

Proof. G acts on a set X where $|X| = p^m = |N|$ by 7.2.6. Let V be a vector space of dimension m over GF(p) and let $\psi: N \to V$ be any $\mathbb{Z}$-isomorphism. If $b \in X$, we can write $b = a\sigma$ with a unique σ in N since N is regular. The rule $b\varphi = \sigma^\psi$ defines a bijection $\varphi: X \to V$. We use this to produce a homomorphism $\Phi: G \to A = \mathrm{Aff}(V)$ as follows: if $\sigma \in N$, let $\sigma^\Phi = (\sigma^\psi)^*$ and if $\pi \in G_a$, let $\pi^\Phi = \psi^{-1}\pi'\psi$ where π' is conjugation in N by π. It is routine to verify that Φ is an isomorphism. Moreover Φ and φ constitute a similarity between G and a subgroup of A containing $N^\Phi = V^*$: to see this one checks that $\varphi\pi^\Phi = \pi\varphi$ when $\pi \in N$ or G_a. □

Combining 7.2.6 and 7.2.7 we come to the conslusion that all soluble primitive permutation groups are to be found among the subgroups of Aff(V) that contain V^*.

Regular Normal Subgroups

We wish to study regular normal subgroups of multiply transitive groups and to show that such normal subgroups are subject to strong restrictions. The key to this theory is an examination of the automorphism group of a group F regarded as a permutation group on the set $F\backslash 1$.

7.2.8. *Let F be a nontrivial finite group and let $G =$* Aut *F act on $F\backslash 1$ in the natural way.*

(i) *If G is transitive, F is an elementary abelian p-group for some prime p.*
(ii) *If G is 2-transitive, either $p = 2$ or $|F| = 3$.*
(iii) *If G is 3-transitive, $||F| = 4$.*
(iv) *G cannot be 4-transitive.*

Proof. (i) Choose any prime p dividing $|F|$. Then F has an element x of order p; by transitivity every element of $F \backslash \{1\}$ is of the form x^α, $\alpha \in G$, and hence of order p. Thus F is a finite p-group and by 1.6.14 its center ζF is nontrivial. Now ζF is characteristic in F and thus is left invariant as a set by G. Transitivity shows that $\zeta F = F$, whence F is an elementary abelian p-group.

(ii) Assume that $p > 2$ and let $1 \neq x \in F$; thus $x \neq x^{-1}$. Suppose that there is an element y of F other than 1, x, or x^{-1}; then 2-transitivity assures us of an α in G such that $(x, x^{-1})\alpha = (x, y)$. But plainly this implies that $y = x^{-1}$. It follows that $F = \{1, x, x^{-1}\}$ and $|F| = 3$.

(iii) If G is 3-transitive on $F \backslash \{1\}$, the latter must have at least three elements and $|F| \geq 4$: also F is an elementary abelian 2-group by (ii). Let $H = \{1, x, y, xy\}$ be a subgroup of F with order 4: assume that there is an element z in $F \backslash H$. Then xz, yz, xyz are distinct elements, so there is an automorphism α in G such that $x^\alpha = xz$, $y^\alpha = yz$, $(xy)^\alpha = xyz$. However, these relations imply that $z = 1$, a contradiction which shows that $H = F$.

(iv) If G were 4-transitive, it would be 3-transitive and $|F \backslash \{1\}| = 3$ by (iii): however this excludes the possibility of 4-transitivity. □

In fact the degree of transitivity is realized in each case (Exercise 7.2.8).

We shall apply this information to regular normal subgroups of multiply transitive groups.

7.2.9. *Let G be a k-transitive permutation group of degree n where $k > 1$. Let N be a nontrivial regular normal subgroup of G.*

(i) *If $k = 2$, then $n = |N| = p^m$ and N is an elementary abelian p-group for some prime p.*
(ii) *If $k = 3$, then either $p = 2$ or $n = 3$.*
(iii) *If $k = 4$, then $n = 4$.*
(iv) *$k \geq 5$ is impossible.*

Proof. We know of course that $1 < k \leq n$. Let G be a permutation group on X with $|X| = n$, and choose a from X. By 7.1.1 the group G_a is $(k - 1)$-transitive on $X \backslash \{a\}$.

The group G_a also acts on the set $N \backslash 1$ by conjugation. Moreover, if $\pi \in N \backslash 1$, then $a\pi \neq a$ by regularity of N. Thus there is a mapping Θ from $N \backslash 1$ to $X \backslash \{a\}$ given by $\pi\Theta = a\pi$: the regularity of N also assures us that Θ is injective. In addition Θ is surjective since N is transitive; thus Θ is a bijection.

If $1 \neq \pi \in N$ and $\sigma \in G_a$, we have $(a\pi)\sigma = a\pi^\sigma$ or $(\pi\Theta)\sigma = (\pi^\sigma)\Theta$. Hence the permutation representations of G_a on $N\backslash 1$ and $X\backslash\{a\}$ are equivalent. Consequently G_a is also $(k-1)$-transitive on $N\backslash 1$ and certainly Aut N must have this property too. The theorem is now a direct consequence of 7.2.8. □

Let us use 7.2.9 to give another proof of the simplicity of the alternating group (see also 3.2.1).

7.2.10. *The alternating group A_n is simple if $n \neq 1, 2$ or 4.*

Proof. We can suppose that $n \geq 5$. Let N be a nontrivial normal subgroup of $G = A_n$. By 7.1.4 the group G is $(n-2)$- and hence 2-transitive; therefore G is primitive by 7.2.4. It follows from 7.2.5 that N is transitive.

We shall prove that $N = G$ by induction on n. Firstly, if $n = 5$, then 5 divides $|N|$ by transitivity, so N contains a 5-cycle, say $\pi = (1, 2, 3, 4, 5)$: if $\sigma = (1, 2, 3)$, then N contains $[\pi, \sigma] = (1, 2, 4)$; however, as in 3.2.1, this leads quickly to $N = G$. Henceforth we suppose that $n > 5$.

By induction on n, the stabilizer G_1, which is isomorphic with A_{n-1}, is simple. Consequently either $N \cap G_1 = 1$ or $G_1 \leq N$. In the first case $N \cap G_a = 1$ for every a, so N is regular: however this contradicts 7.2.9 since $n - 2 \geq 4$. Finally, if $G_1 \leq N$, then $G_1 = N_1$ and transitivity yields $|G : G_1| = n = |N : N_1| = |N : G_1|$. Therefore $|N| = |G|$ and $N = G$. □

Exercises 7.2

1. Prove that S_n is primitive.
2. Let H and K be permutation groups acting transitively on sets X and Y respectively. Prove that the wreath product $H \wr K$ is imprimitive if $|X| > 1$ and $|Y| > 1$.
3. Find all primitive permutation groups of degree at most 5.
4. Let G be a nilpotent permutation group $\neq 1$. Prove that G is primitive if and only if the order and degree of G equal a prime.
5. Let G be a supersoluble permutation group $\neq 1$. If G is primitive, show that it is similar to a subgroup of Aff(GF(p)) containing the translation group for some prime p. Conversely show that any such group is supersoluble and primitive. How many similarity types are there for a given p?
6. Prove that Aff(GF(p)) $= H(p)$ where p is prime.
7. Complete the proof of 7.2.7 by showing that Φ is an isomorphism and (Φ, φ) is a similarity.
8. Prove the converse of 7.2.8 by showing that all the given degrees of transitivity actually occur.

9. If G is a primitive permutation group with even degree > 2, prove that 4 divides $|G|$. [*Hint*: Use Exercise 1.6.19.]

10. Let G be a permutation group which contains a minimal normal subgroup that is transitive and abelian. Then G is primitive.

11. Let F be a finite group and let $G = \text{Aut}\, F$ act on $F \backslash \{1\}$. Prove that G is primitive if and only if either F is an elementary abelian 2-group or $|F| = 3$.

12. If G is a soluble transitive permutation group of prime degree p, then G is similar to a subgroup of $\text{Aff}(\text{GF}(p))$ containing the translation group.

13. Let G be a transitive permutation group of prime degree p and let P be a Sylow p-subgroup.
    (a) Show that $|P| = p$ and $N_G(P)/P$ is cyclic of order dividing $p - 1$.
    (b) Either $|G| = p$ or G' is simple and G' is the only minimal normal subgroup of G. [*Hint*: If N is minimal normal in G, show that $P \leq N$ and apply the Frattini argument.]

14. Let G be a k-transitive permutation group of degree n where $k > 1$. Assume G is not similar to S_n. Let $N \lhd G$ be nontrivial and nonregular. Prove that N is $(k - 1)$-transitive. [*Hint*: Let G be a counterexample with k minimal. Let G act on X and let $a \in X$. Argue that N_a is regular and $k \geq 4$. Invoke 7.2.9 to show that $|N_a|$ is a power of 2. Find an element $\sigma = (a)(b, c)(d, e)\cdots$ in N_a and let $\pi \in G$ map (a, b, c) to (d, b, c). Consider $[\sigma, \pi]$ to get a contradiction.]

15. Let G be a k-transitive permutation group of degree n, not similar to S_n, and let $k > 3$. Prove that every nontrivial normal subgroup is $(k - 1)$-transitive.

16. Let G be a k-transitive permutation group where $k > 2$. Prove that every nontrivial normal subgroup is $(k - 2)$-transitive with the sole exception when G is similar to S_4 and $|N| = 4$.

7.3. Classification of Sharply k-Transitive Permutation Groups

By definition a sharply 1-transitive permutation group is just a regular group. Since every group has a faithful regular representation, one cannot expect to be able to say anything about the structure of sharply 1-transitive groups.

While sharply 2-transitive groups are still numerous, they are subject to severe restrictions, as we see from the next result.

7.3.1. *Let G be a sharply 2-transitive permutation group. Then the degree of G is p^m for some prime p, and G has a normal Sylow p-subgroup. Moreover G is similar to a subgroup of* Aff(V) *which contains the translation group, V being a vector space of dimension m over* GF(p).

Proof. Let G act on a set X with $|X| = n$. We denote by $G(0)$ and $G(1)$ the sets of permutations in G that have no fixed points and exactly one fixed point respectively. Then, because G is sharply 2-transitive, $G = 1 \cup G(0) \cup G(1)$.

Let p be any prime dividing n. Since $|G|$ must equal $n(n-1)$, there is an element π of order p in G; naturally π involves 1-cycles and p-cycles only. Hence, if r is the number of 1-cycles in π, we have $n \equiv r \bmod p$. Since p divides n, it follows that $r = 0$ and $\pi \in G(0)$. Next $G(1)$ is the union of the disjoint subsets $G_a \backslash 1$, $a \in X$. This implies that $|G(1)|$ equals $n(|G_a| - 1) = n(n-2)$ because $|G_a| = |G|/n = n - 1$. Consequently $|G(0)| = n(n-1) - n(n-2) - 1 = n - 1$.

Next, for any a in X we have $G_a \cap G_a^\pi = G_a \cap G_{a\pi} = 1$ since $\pi \in G(0)$. It follows that $G_a \cap C_G(\pi) = 1$ and

$$|G : C_G(\pi)| \geq |G_a C_G(\pi) : C_G(\pi)| = |G_a| = n - 1.$$

Therefore π has at least $n - 1$ conjugates in G, all of which belong to $G(0)$. However $|G(0)| = n - 1$, so these conjugates constitute the whole set $G(0)$. Since this conclusion applies to every prime divisor of n, we deduce that n must be a power of the prime p, say $n = p^m$.

The order of G is $p^m(p^m - 1)$ and G has a Sylow p-subgroup P of order p^m. Now $P \backslash 1 \subseteq G(0)$ by the argument that led to $\pi \in G(0)$. Since $|G(0)| = n - 1 = p^m - 1 = |P \backslash 1|$, it follows that $P = G(0) \cup 1$. The evident fact that $\sigma^{-1} G(0) \sigma = G(0)$ for all σ in G implies that $P \lhd G$. Finally we choose a minimal normal subgroup N of G contained in P and observe that N is abelian since $\zeta N \neq 1$: now apply 7.2.6 and 7.2.7 to obtain the result. □

According to a deep result of Zassenhaus either a sharply 2-transitive permutation group is similar to a group of transformations of $F = \mathrm{GF}(p^m)$ of the form $x \mapsto ax^\sigma + b$ where $0 \neq a$, $b \in \mathrm{GF}(p^m)$ and σ is an automorphism of F, or the degree is 5^2, 7^2, 11^2, 23^2, 29^2, or 59^2. Zassenhaus has also proved that every sharply 3-transitive permutation group is similar to $L(p^m)$ or $M(p^m)$. Proofs of these results may be found in [b50].

Sharply k-Transitive Groups for $k \geq 4$

If $k \geq 4$, there are, apart from alternating and symmetric groups, sharply k-transitive groups in two cases only, $k = 4$ and $k = 5$. Moreover there are up to similarity only two examples, the celebrated Mathieu groups M_{11} and M_{12}, which have degrees 11 and 12 respectively. This remarkable result was published by Jordan in 1872. Our aim in the remainder of this section is to prove Jordan's theorem; M_{11} and M_{12} will be constructed in 7.4.

Let us begin with a lemma which will enable us to eliminate certain possibilities for sharp k-transitivity.

7.3.2. *Let G be a k-transitive permutation group on a set X and let Y be a subset of X containing k elements. Denote by H the stabilizer of Y in G and let P be a Sylow p-subgroup of H. Then $N_G(P)$ is k-transitive on the set of fixed points of P.*

Proof. In the first place $N_G(P)$ does act on the set of fixed points of P: for if $\pi \in N_G(P)$, $\sigma \in P$ and b is a fixed point of P, then $(b\pi)\sigma = (b\sigma^{\pi^{-1}})\pi = b\pi$ and $b\pi$ is a fixed point of P.

Let $Y = \{a_1, \ldots, a_k\}$; observe that the a_i are fixed points of P because $P \leq H$. It is therefore enough to prove that if $b_1, \ldots, b_k$ are fixed points of P, there is a π in $N_G(P)$ such that $a_i\pi = b_i$, $i = 1, 2, \ldots, k$.

By k-transitivity of G we can find σ in G with the property $a_i = b_i\sigma$, $i = 1, 2, \ldots, k$. Since b_i is fixed by P, one sees that a_i is a fixed point of the group $\sigma^{-1}P\sigma$, from which it follows that $\sigma^{-1}P\sigma \leq H$. By Sylow's Theorem $\sigma^{-1}P\sigma = \tau^{-1}P\tau$ for some τ in H, whence $\pi = \tau\sigma^{-1} \in N_G(P)$. Finally $a_i\pi = (a_i\tau)\sigma^{-1} = a_i\sigma^{-1} = b_i$ for $i = 1, 2, \ldots, k$, as required. □

This result will now be used to exclude two possibilities for sharp k-transitivity.

7.3.3. *There are no sharply* 4*-transitive permutation groups of degree* 10; *nor are there any sharply* 6*-transitive groups of degree* 13.

Proof. (i) Suppose that G is in fact a sharply 4-transitive group of degree 10. By 7.1.3 the order of G is $10 \cdot 9 \cdot 8 \cdot 7$ and thus a Sylow 7-subgroup P of G is cyclic of order 7. For convenience we shall assume that $G \leq S_{10}$ and P is generated by $\pi = (1, 2, 3, 4, 5, 6, 7)$. Applying 7.3.2 with $k = 3$, X the set of integers $1, 2, \ldots, 10$ and $Y = \{8, 9, 10\}$, we conclude that $N = N_G(P)$ is 3-transitive on Y—note here that $P \leq G_Y$. This action therefore yields an *epimorphism* $\varphi: N \to \operatorname{Sym} Y$. Writing $C = C_G(P)$, we have $C \lhd N$ and N/C abelian since $\operatorname{Aut} P$ is abelian. Hence $C^\varphi \geq (N^\varphi)'$, which has order 3. It follows that C contains an element σ of order 3. Now $\sigma\pi = \pi\sigma$, so $\pi\sigma$ has order 21 and must be a product of a 7-cycle and a 3-cycle. Hence $(\pi\sigma)^7$ is non-trivial and fixes seven points, which contradicts the sharp 4-transitivity of G.

(ii) Now suppose that G is sharply 6-transitive with degree 13: in this case $|G| = 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ and there is an element π of G with order 5 which generates a Sylow 5-subgroup P. Of course π involves 1-cycles and 5-cycles only and, since it cannot fix $13 - 5 = 8$ points, it must contain exactly two 5-cycles. We may assume that $G \leq S_{13}$ and $\pi = (1, 2, 3, 4, 5)(6, 7, 8, 9, 10)$. Apply 7.3.2 with $k = 3$, X the set of integers $1, 2, \ldots, 13$ and $Y = \{11, 12, 13\}$; then $N = N_G(P)$ is 3-transitive on Y. Just as in (i) we argue that $C_G(P)$ contains an element σ of order 3. Then $\pi\sigma$ has order 15 and must involve 5-cycles and 3-cycles. In fact, since $(\pi\sigma)^6 = \pi^6 = \pi$, there are exactly two 5-cycles and one 3-cycle in π. But then $(\pi\sigma)^5$ is a 3-cycle and fixes ten points, a contradiction. □

Jordan's Theorem on Multiply Transitive Groups

We are now in a position to undertake the proof of the following major result.

7.3.4 (Jordan). *Assume that $k \geq 4$ and let G be a sharply k-transitive permutation group of degree n which is of neither symmetric nor alternating type. Then either $k = 4$* and *$n = 11$ or $k = 5$ and $n = 12$.*

Proof. We shall suppose throughout that $G \leq S_n$.

(i) *If $k = 4$, then $n \geq 8$ and all elements of order 2 are conjugate in G.* In the first place $n \geq k = 4$ and $|G| = n(n-1)(n-2)(n-3)$. If $n = 4$ or 5, then $|G| = n!$ and $G = S_n$. If $n = 6$, then $|G| = \frac{1}{2}(n!)$ and $G = A_n$. Hence $n \geq 7$.

Next suppose that $n = 7$; then $|G| = 7!/6$ and G has index 6 in S_7. By 1.6.9 the core of G in S_7 has index dividing 6! and hence is a proper nontrivial normal subgroup of S_7. But A_7 is the only such subgroup and its index is 2, so $|S_7 : G| \leq 2$, a contradiction which shows that $n \geq 8$.

Consider two elements π and σ of G with order 2. Each of these can fix at most three points and must therefore involve at least two 2-cycles, say $\pi = (1, 2)(3, 4)\dots$ and $\sigma = (a, b)(c, d)\dots$. By 4-transitivity there is a τ in G such that $(1, 2, 3, 4)\tau = (a, b, c, d)$. Then $\pi^\tau = (a, b)(c, d)\dots$. Hence $\sigma^{-1}\pi^\tau$ fixes a, b, c, d, and by sharp 4-transitivity $\pi^\tau = \sigma$, as required.

(ii) *If $k = 4$, then $n = 11$* (the main step in the proof). Using 4-transitivity we can find in G permutations of the form $\pi = (1)(2)(3, 4)\dots$ and $\sigma = (1, 2)(3)(4)\dots$. Since π^2 and σ^2 both fix 1, 2, 3, and 4 we may be sure from sharp 4-transitivity that $\pi^2 = 1 = \sigma^2$. Moreover $\pi\sigma$ and $\sigma\pi$ agree on $\{1, 2, 3, 4\}$, so $\pi\sigma = \sigma\pi$ for the same reason. Hence

$$H = \langle \pi, \sigma \rangle$$

is a Klein 4-group.

The permutation π can have at most one fixed point in addition to 1 and 2. It is convenient to denote this hypothetical third fixed point by 7; however it should be borne in mind that the fixed point 7 may not exist, in which case statements about 7 are to be ignored.

Since $\pi\sigma = \sigma\pi$, the permutation σ permutes $\{1, 2, 7\}$, the set of fixed points of π. Because σ interchanges 1 and 2, it must fix 7. Now consider $\tau = \pi\sigma$. Then (i) shows that τ is conjugate to π and, in consequence, has the same number of fixed points. Among the latter will be 7—if it exists—since π and σ fix 7. Hence τ has two further fixed points. Noting that τ interchanges 1 and 2 and also 3 and 4, we may suppose that the remaining fixed points of τ are 5 and 6. Again π permutes $\{5, 6, 7\}$, the set of fixed points of τ, so π must interchange 5 and 6, as does σ by the same argument. The

situation is, therefore, the following:

$$\pi = (1)(2)(3, 4)(5, 6)(7)\ldots, \qquad \sigma = (1, 2)(3)(4)(5, 6)(7)\ldots,$$

and

$$\tau = (1, 2)(3, 4)(5)(7)\ldots.$$

The next point to establish is that $H = C_G(H)$. Let $1 \neq \rho \in C_G(H)$. Since ρ commutes with each of π, σ, τ, it permutes each of the sets of fixed points of these permutations, namely $\{1, 2, 7\}$, $\{3, 4, 7\}$, and $\{5, 6, 7\}$. Hence $7\rho = 7$ and ρ has the form

$$\rho = (1, 2)^r(3, 4)^s(5, 6)^t(7)\ldots$$

where $r, s, t = 0$ or 1. Since ρ can fix no more than three points, at least two of r, s, t equal 1. If $r = s = t = 1$ (so that $\rho = (1, 2)(3, 4)(5, 6)(7)\ldots$), then $\pi\rho$ fixes 3, 4, 5, and 6, which is impossible. Hence exactly two of r, s, t equal 1. If $t = 0$, then $r = 1 = s$ and ρ and τ agree on $\{1, 2, 3, 4\}$, and $\rho = \tau$ by sharp 4-transitivity. Similarly the cases $r = 0$ and $s = 0$ lead to $\rho = \pi$ and $\rho = \sigma$ respectively. Hence $\rho \in H$ in all cases and $C_G(H) \leq H$. However H is abelian, so $H \leq C_G(H)$ and $H = C_G(H)$.

The set $\{1, 2, 3, 4, 5, 6, 7\}$ is visibly a union of H-orbits and it includes all fixed points of nontrivial permutations in H. Since $n \geq 8$, there is at least one further H-orbit, say X. No nontrivial element of H may fix a point of X, which shows that H acts regularly on X and consequently X has exactly four elements. Let S be the subgroup of permutations in G that leave X fixed *as a set*. Then, since G is 4-transitive, S induces all 4! permutations of X. Also no nontrivial element of S may fix every point of X, so $S \simeq S_4$. Now $H \leq S$ since X is an H-orbit, and there is only one regular subgroup of S_4 that is a Klein 4-group, namely, the subgroup consisting of 1 and the three permutations of the form $(i, j)(k, l)$. Hence $H \lhd S$ and $S \leq N_G(H) = N$ say. Now $|N : H| = |N_G(H) : C_G(H)| \leq |\text{Aut } H| = 6$. Therefore $|N| \leq 24$ and it follows that $N = S$. Thus S is independent of the H-orbit X.

Let $X = \{i, j, k, l\}$; then there is a permutation ξ in S which acts on X like $(ij)(k)(l)$ since S induces all 4! permutations on X. Suppose that $X' = \{i', j', k', l'\}$ is another H-orbit not contained in $\{1, 2, 3, 4, 5, 6, 7\}$. Now S fixes X' setwise and $\xi^2 = 1$, so ξ must act on X' like $(i', j')(k', l')$, say, since it cannot fix four points. But H acts regularly on X', so some $\eta \in H$ produces the permutation $(i', j')(k', l')$. Then $\xi\eta^{-1}$ must be trivial, and $\xi = \eta \in H$, which is impossible since a nontrivial element of H cannot fix k and l.

It follows that X is the only H-orbit not contained in $\{1, 2, 3, 4, 5, 6, 7\}$. Therefore $n = 6 + 4 = 10$ or $n = 7 + 4 = 11$ (since "7" may not exist). By 7.3.3 the first case is impossible, so $n = 11$.

(iii) *Final step.* We assume that $k \geq 5$ and use induction on k to complete the proof. If a is any element of the permuted set Y, the stabilizer G_a is $(k - 1)$-transitive on $Y \backslash \{a\} = T$ by 7.1.1. Indeed G_a is *sharply* $(k - 1)$-transitive on T, as we see from its order $|G|/n$. If $|G_a| = (n - 1)!$ or $\frac{1}{2}((n - 1)!)$, then

$|G| = n|G_a| = n!$ or $\frac{1}{2}(n!)$ and $G = S_n$ or A_n, contrary to assumption. Hence G_a is neither a symmetric nor an alternating group. By induction hypothesis $k - 1 = 4$ or 5, and $k = 5$ or 6. Moreover, should k be 5, then $n - 1 = 11$ and $n = 12$. If however $k = 6$, then $n - 1 = 12$ and $n = 13$, a combination that has been seen to be impossible in 7.3.3. The proof is now complete. □

EXERCISES 7.3

1. A sharply 3-transitive permutation group has degree $p^m + 1$ where p is prime. Show also that all such degrees occur.
2. Let G be a k-transitive permutation group of degree n which is neither alternating nor symmetric. Assume that $k > 5$. Prove that $(n - k)! \geq 2n$. Deduce that $k \leq n - 4$.
3. Let k be a positive integer and let G be a permutation group of smallest order subject to G being k-transitive. Prove that G is sharply k-transitive. [*Hint*: Use 7.3.2.]
4. If G is a soluble 3-transitive permutation group, then G is similar to S_3 or S_4. [*Hint*: Identity G with a subgroup of Aff(V) where V is a vector space of dimension m over GF(p). Let N be minimal normal in G_0: prove that N acts irreducibly on V and use Schur's Lemma (8.1.4) to show that V can be identified with a field F of order p^m and N with F^*. Now argue that $|G_0| \leq m(p^m - 1)$ and deduce that $p^m = 3$ or 4.]
5. Suppose that G is a finite insoluble group whose proper subgroups are soluble. Prove that G has no permutation representation as a 4-transitive group.

7.4. The Mathieu Groups

To complement Jordan's theorem we shall construct two permutation groups which are sharply 4-transitive of degree 11 and sharply 5-transitive of degree 12. These groups were discovered by Mathieu in 1861.

We shall employ a method of construction due to Witt which involves two simple, if technical, lemmas.

7.4.1. *Let H be a permutation group on a set Y and let G be a subgroup and π an element of H such that $H = \langle \pi, G \rangle$. Write $Y = X \cup \{a\}$ where $a \notin X$. Assume that G fixes a and acts k-transitively on X where $k \geq 2$ and $a\pi \neq a$. Assume further that there exist σ in G and b in X such that $b\sigma \neq b$, $\pi^2 = \sigma^2 = (\pi\sigma)^3 = 1$ and $G_b^\pi = G_b$. Then H is $(k + 1)$-transitive on Y and $H_a = G$.*

Proof. Let $K = G \cup (G\pi G)$; then $K^{-1} = K$ because $\pi^2 = 1$. Let $\tau \in G \backslash G_b$, so that $b\tau \neq b$. Since $k \geq 2$, we deduce from 7.1.1 that G_b acts transitively on $X \backslash \{b\}$. Hence there exists a ρ in G_b such that $(b\tau)\rho = b\sigma$ and thus $\tau\rho\sigma^{-1} \in$

G_b or $\tau\rho \in G_b\sigma$. It follows that $\tau \in G_b\sigma G_b$ and hence that

$$G = G_b \cup (G_b\sigma G_b). \tag{4}$$

Now the relations $\pi^2 = \sigma^2 = (\pi\sigma)^3 = 1$ imply that $\pi\sigma\pi = \sigma\pi\sigma$. Consequently we obtain from (4)

$$\pi G\pi = (\pi G_b\pi) \cup (\pi G_b\sigma G_b\pi) = G_b^\pi \cup (G_b^\pi(\pi\sigma\pi)G_b^\pi)$$
$$= G_b \cup (G_b(\sigma\pi\sigma)G_b) \subseteq G \cup (G\pi G) = K.$$

It follows that $KK \subseteq K$ and K is a subgroup. Since $\pi \in K$ and $G \leq K$, we have $H = \langle \pi, G\rangle \leq K$ and hence $H = K = G \cup (G\pi G)$.

By hypothesis G is transitive on X and $a\pi \neq a$. It follows that H is transitive on $Y = X \cup \{a\}$. Moreover, since G fixes a and $a\pi \neq a$, no element of $G\pi G$ can fix a. Hence $H_a = G$, which is k-transitive on $Y \backslash \{a\} = X$. By 7.1.1 the group H is $(k + 1)$-transitive on Y. □

The second technical lemma is a consequence of 7.4.1. It tells us how to construct 5-transitive groups, starting with a 2-transitive group.

7.4.2. *Let G be a subgroup of S_n where $n \geq 5$. Assume that G fixes 1, 2, and 3 and is 2-transitive on $T = \{4, 5, \dots, n\}$. Let σ in G have order 2 and let $c\sigma \neq c$ for some c in T. Consider three permutations of order 2 in S_n of the form*

$$\pi_1 = (1, c)(2)(3)\dots, \qquad \pi_2 = (1, 2)(3)(c)\dots, \qquad \pi_3 = (2, 3)(1)(c)\dots$$

(where nothing is known about other cycles); assume that

$$(\pi_1\sigma)^3 = (\pi_2\pi_1)^3 = (\pi_3\pi_2)^3 = 1,$$
$$(\sigma\pi_2)^2 = (\sigma\pi_3)^2 = (\pi_1\pi_3)^2 = 1,$$

and also that $G_c^{\pi_1} = G_c^{\pi_2} = G_c^{\pi_3} = G_c$. Then the group $H = \langle \pi_1, \pi_2, \pi_3, G\rangle$ is 5-transitive on $\{1, 2, \dots, n\}$ and G is the stabilizer of $\{1, 2, 3\}$ in H.

Proof. Apply 7.4.1 to $K = \langle \pi_1, G\rangle$ with $k = 2$, $a = 1$, $b = c$, and $X = T$. Thus K is 3-transitive on $T \cup \{1\}$ and $K_1 = G$.

Next G acts primitively on T since it is 2-transitive (7.2.4). Consequently G_c is maximal in G by 7.2.3 and $G = \langle \sigma, G_c\rangle$ in view of $c\sigma \neq c$. Now the relations $\sigma^2 = (\sigma\pi_2)^2 = \pi_2^2 = 1$ imply that $\sigma\pi_2 = \pi_2\sigma$. Therefore $(K_1)^{\pi_2} = G^{\pi_2} = \langle \sigma, G_c^{\pi_2}\rangle = \langle \sigma, G_c\rangle = G = K_1$. We are now in a position to apply 7.4.1 again, this time to $L = \langle \pi_2, K\rangle$ with $k = 3$, $a = 2$, $b = 1$, $X = T \cup \{1\}$, and π_1 instead of σ. The conclusion is that L is 4-transitive on $T \cup \{1, 2\}$ and $L_2 = K$.

The given relations also imply that $\pi_1\pi_3 = \pi_3\pi_1$ and $\sigma\pi_3 = \pi_3\sigma$. Hence

$$K^{\pi_3} = \langle \pi_1, G^{\pi_3}\rangle = \langle \pi_1, \sigma, G_c^{\pi_3}\rangle = \langle \pi_1, \sigma, G_c\rangle = K$$

and $(L_2)^{\pi_3} = L_2$. We apply 7.4.1 to $H = \langle \pi_3, L\rangle$ with $k = 4$, $a = 3$, $b = 2$, $X = T \cup \{1, 2\}$ and π_2 in place of σ, the conclusion being that $H = \langle \pi_3, L\rangle$

is 5-transitive on $X \cup \{1, 2, 3\} = \{1, 2, 3, \dots, n\}$ and $H_3 = L$. Finally $H_{\{1,2,3\}} = L_{\{1,2\}} = K_1 = G$. □

The Groups M_{11} and M_{12}

In order to exploit 7.4.2 we have to realize the situation envisaged there. This involves a careful choice of permutations.

7.4.3. *Let* $X = \{1, 2, 3, \dots, 11, 12\}$ *and consider the following seven permutations of* X:

$$\varphi = (4, 5, 6)(7, 8, 9)(10, 11, 12),$$
$$\chi = (4, 7, 10)(5, 8, 11)(6, 9, 12),$$
$$\psi = (5, 7, 6, 10)(8, 9, 12, 11),$$
$$\omega = (5, 8, 6, 12)(7, 11, 10, 9),$$
$$\pi_1 = (1, 4)(7, 8)(9, 11)(10, 12),$$
$$\pi_2 = (1, 2)(7, 10)(8, 11)(9, 12),$$
$$\pi_3 = (2, 3)(7, 12)(8, 10)(9, 11).$$

(i) *The group* $M_{12} = \langle \varphi, \chi, \psi, \omega, \pi_1, \pi_2, \pi_3 \rangle$ *is sharply* 5*-transitive of degree* 12 *on the set* X; *its order is* $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95{,}040$.
(ii) *The group* $M_{11} = \langle \varphi, \chi, \psi, \omega, \pi_1, \pi_2 \rangle$ *is the stabilizer of* 3 *in* M_{12}; *it is sharply* 4*-transitive of degree* 11 *on* $X \backslash \{3\}$ *and has order* $11 \cdot 10 \cdot 9 \cdot 8 = 7920$.

Proof. One easily verifies that $E = \langle \varphi, \chi \rangle$ is an elementary abelian group of order 9 which acts regularly on $X \backslash \{1, 2, 3\}$. Also $\psi^2 = \omega^2$ has order 2 and $\psi^{-1}\omega\psi = \omega^{-1}$; this shows that $Q = \langle \psi, \omega \rangle$ is a quaternion group of order 8 (see 5.3). Straightforward calculations reveal that $\psi^{-1}\varphi\psi = \chi$, $\omega^{-1}\varphi\omega = \varphi\chi$, $\psi^{-1}\chi\psi = \varphi^{-1}$, and $\omega^{-1}\chi\omega = \omega\chi^{-1}$. Therefore Q normalizes E and $G = QE$ is a group of order $8 \cdot 9 = 72$.

Next we observe that Q fixes 4, whereas no nontrivial element of E has this property; therefore $G_4 = G_4 \cap (QE) = QE_4 = Q$. A glance at the permutations that generate Q should convince the reader that Q acts transitively on $\{5, 6, 7, 8, 9, 10, 11, 12\}$. Hence G is transitive on $\{4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Since $G_4 = Q$, we conclude via 7.1.1 that G is 2-transitive on this nine-element set. Moreover this is sharp 2-transitivity because $|G| = 9 \cdot 8$.

Now apply 7.4.2 with $n = 12$, $c = 4$ and

$$\sigma = \varphi^{-1}\psi^2\varphi = (4, 6)(7, 12)(8, 11)(9, 10);$$

of course one must at this point check that the equations of 7.4.2 hold and that π_1, π_2, π_3 normalize $G_4 = Q$, but this is routine. The conclusion is that $M_{12} = \langle \pi_1, \pi_2, \pi_3, G \rangle$ is 5-transitive of degree 12 and that G is the stabi-

lizer of $\{1, 2, 3\}$ in M_{12}. We saw that G is sharply 2-transitive on $\{4, 5, \ldots, 11, 12\}$; consequently the stabilizer of $\{1, 2, 3, 4, 5\}$ in M_{12} is 1 and M_{12} is sharply 5-transitive.

From the proof of 7.4.2 (last line) the stabilizer of 3 in M_{12} is M_{11}. Now 7.1.1 shows that M_{11} is 4-transitive on $X \backslash \{3\}$. The stabilizer of $\{1, 2, 4, 5\}$ in M_{11} equals that of $\{1, 2, 3, 4, 5\}$ in M_{12}, which is 1. Hence M_{11} is sharply 4-transitive of degree 11. The statements about orders follow from 7.1.3. □

It can be shown—altnough we shall not take the matter up here—that *to within similarity M_{11} is the only sharply 4-transitive group of degree* 11 *and M_{12} the only sharply 5-transitive group of degree* 12. For details see [b50].

The Mathieu Groups M_{22}, M_{23}, M_{24}

There are three further Mathieu groups. M_{24} is a 5-transitive permutation group of degree 24 and order 244,823,040. It can be constructed with the aid of 7.4.2 in a manner akin to that employed for M_{12}: the starting point is the group $G = \mathrm{PSL}(3, 4)$, which acts 2-transitively on the twenty-one 1-dimensional subspaces of a 3-dimensional vector space over GF(4). The Mathieu group M_{23} appears as the stabilizer of an element in M_{24} and the group M_{22} is the stabilizer of a two-element set in M_{24}. Thus M_{23} is 4-transitive with degree 23 and order 10,200,960 and M_{22} is 3-transitive of degree 22 and order 443,520. Of course none of these groups is sharply transitive, by consideration of order. Further details can be found in [b50]

Simplicity of the Mathieu Groups

The five Mathieu groups have a notable property—they are all simple. Indeed these groups are examples of sporadic simple groups, not occurring in an infinite sequence of simple groups.

We shall content ourselves with proving the simplicity of M_{11} and M_{12}.

7.4.4. *The groups M_{11} and M_{12} are simple.*

Proof. (i) Let $G = M_{11}$ and suppose that N is a proper nontrivial normal subgroup of G: then we can choose N to be a minimal subgroup of this type. Since G is 4-transitive, it is primitive (7.2.4) and therefore N is transitive (7.2.5). It follows that $|N|$ is divisible by 11. Now $|G| = 11 \cdot 10 \cdot 9 \cdot 8$, so N contains a Sylow 11-subgroup of G, say P; clearly P is generated by an 11-cycle, say π, and P is transitive.

We claim that $P = C_G(P)$. To see this let $\tau \in C_G(P)$ and consider $A = \langle \tau, P \rangle$. Now A is certainly abelian and it is also transitive since P is. Therefore A is regular and its order must be 11. Hence $|P| = |A|$ and $\tau \in P$, which establishes our claim.

Next consider $L = N_G(P)$: we shall show that L has odd order. If this is false, L contains an element σ of order 2. Now σ must have at least one fixed point, the degree being 11, and there is nothing to be lost in supposing σ to fix 1; for, G being transitive, we can always replace P by a suitable conjugate. Since $P = C_G(P)$, the permutation σ must induce by conjugation in P an automorphism of order 2. But Aut P is a cyclic group of order 10 and it has exactly one element of order 2, the automorphism $x \mapsto x^{-1}$. Hence $\pi^\sigma = \pi^{-1}$. Consequently $1\pi^i\sigma = 1\sigma\pi^{-i} = 1\pi^{-i} \neq 1\pi^i$ if $1 \leq i < 11$. Since σ has only 1-cycles and 2-cycles, these considerations show that σ must consist of (1) and five 2-cycles. But this forces σ to be an odd permutation, whereas $G \leq A_{12}$ because all of the generating permutations of M_{12} are even. By this contradiction L had odd order.

Combining the result of the last paragraph with the fact that $|L:P| = |N_G(P):C_G(P)|$ divides $|\text{Aut } P| = 10$, we conclude that $|L:P| = 1$ or 5. Now the Frattini argument (5.2.14) shows that $G = NN_G(P) = NL$, which implies that $L \nleq N$. Since $P \leq N \cap L \leq L$ and $|L:P| = 1$ or 5, we must have $N \cap L = P$, that is, P is self-normalizing in N.

At this point we can apply a theorem of Burnside (10.1.8), concluding that elements of N with order prime to 11 form a subgroup; this subgroup must necessarily be normal in G, whence it is trivial by minimality of N. It follows that $P = N \lhd G$ and $L = G$, which is impossible because $|L:P| \leq 5$.

However, the reader who does not wish to appeal to an unproved theorem may argue directly, as indicated in Exercise 7.4.3 below.

(ii) Consider now $H = M_{12}$ and suppose that N is a proper nontrivial normal subgroup of H. Then $G \cap N \lhd G$ and either $G \cap N = 1$ or $G \leq N$ because G is simple. Since H is primitive and G is the stabilizer of 3 in H, we conclude via 7.2.3 that G is maximal in H. If $G \leq N$, then $G = N$ and $H_3 = G \lhd H$; however this would mean that G fixed every point, not merely 3, and $G = 1$. Hence $G \cap N = 1$, and also $H = GN$ by the maximality of G. Next, $C_G(N) \lhd G$, so either $C_G(N) = 1$ or $[N, G] = 1$; however the latter implies that $G \lhd GN = H$, which has been seen to be false. Hence $C_G(N) = 1$ and $|G| \leq |\text{Aut } N|$. Also $|N| = |H:G| = 12$. However, no group of order 12 can have its automorphism group of order as large as $|G| = 7920$—by Exercise 1.5.16. Thus our proof is complete. □

Exercises 7.4

1. A sharply 2-transitive permutation group of order > 2 cannot be simple, whereas there are infinitely many sharply 3-transitive groups that are simple.
2. Prove that M_{11} is a maximal subgroup of M_{12}.
3. Complete the proof of 7.4.4 without appealing to Burnside's theorem. [*Hint*: N is 3-transitive by Exercise 7.2.15.]
4. Prove that the Sylow 2-subgroups of M_{11} are semidihedral of order 16.

CHAPTER 8

Representations of Groups

The aim of this chapter is to introduce the reader to the theory of representations of groups by linear transformations of a vector space or, equivalently, by matrices over a field. Aside from its intrinsic interest this theory has proved to be a most powerful tool for studying finite groups.

8.1. Representations and Modules

Let G be a group, F a field, and V a vector space over F. A homomorphism ρ from G to $\mathrm{GL}(V)$, the group of all nonsingular linear transformations of V, is called a *linear representation* of G over F, or simply an *F-representation* of G. Here we shall always assume that the dimension n of V is finite; the integer n is known as the *degree* of ρ. If $\mathrm{Ker}\ \rho = 1$, then ρ is called *faithful*.

Suppose that $\{v_1, \ldots, v_n\}$ is an (ordered) basis of V. Then if $g \in G$, there is a matrix $g^{\rho*}$ in $\mathrm{GL}(n, F)$ which represents the linear transformation g^ρ with respect to the basis. The mapping $\rho^*: G \rightarrow \mathrm{GL}(n, F)$ is a homomorphism which will be called the *associated matrix representation* with respect to the given basis. If $(g)\rho_{ij}$ denotes the (i, j) entry of $g^{\rho*}$, then in fact

$$v_i g^\rho = \sum_{j=1}^{n} (g)\rho_{ij}\, v_j.$$

An obvious example of an F-representation is the *trivial representation* $\iota(G)$: $G \rightarrow F$, which maps each element of G to 1_F: of course, this has degree 1.

More interesting representations may be constructed from permutation representations. Let $\pi: G \rightarrow \mathrm{Sym}\ X$ be a permutation representation of G on

a finite set X, and let V be a vector space over F with basis $\{v_x | x \in X\}$. Define $g^\rho \in \mathrm{GL}(V)$ by writing $v_x g^\rho = v_{xg^\pi}$: one easily checks that ρ is a linear representation of degree $|X|$. Notice that the matrix representing g^ρ with respect to the given basis is just the permutation matrix associated with the permutation g^π.

Usually one identifies the permutation representation π with the corresponding F-representation ρ, so that a permutation representation may be thought of as a special type of linear representation.

Group Rings and Group Algebras

If G is a group and R is any ring with an identity element, the *group ring*

$$RG$$

is defined to be the set of all formal sums $\sum_{x \in G} r_x x$ where $r_x \in R$ and $r_x = 0$ with finitely many exceptions, together with the rules of addition and multiplication

$$\left(\sum_x r_x x\right) + \left(\sum_x r'_x x\right) = \sum_x (r_x + r'_x)x$$

and

$$\left(\sum_x r_x x\right)\left(\sum_x r'_x x\right) = \sum_x \left(\sum_{yz=x} r_y r'_z\right)x.$$

It is very simple to verify that with these rules RG is a ring with identity element $1_R 1_G$, which is written simply 1.

If F is a field, then FG, in addition to being a ring, has a natural F-module structure given by

$$f\left(\sum_x f_x x\right) = \sum_x (ff_x)x, \qquad (f \in F).$$

Thus FG is a vector space over F. In addition we have $f(uv) = (fu)v = u(fv)$ where $f \in F$ and $u, v \in FG$. Thus FG is an *F-algebra*, known as the *group algebra* of G over F.

It would be hard to overestimate the importance of group rings in the theory of groups. For the present let us explain how the group algebra is inescapably involved in the study of F-representations.

Suppose that $\rho: G \to \mathrm{GL}(M)$ is an F-representation of G with degree n. Then M can be turned into a right FG-module by means of the rule

$$a\left(\sum_{x \in G} f_x x\right) = \sum_{x \in G} f_x(ax^\rho), \qquad (a \in M).$$

Verification of the module axioms is very simple. Conversely, if M is any right FG-module with finite F-dimension n, there is a corresponding F-

representation $\rho: G \to \mathrm{GL}(M)$ of degree n given by

$$ag^\rho = ag, \qquad (a \in M).$$

A few moments reflection should convince the reader that what we have here is nothing less than a bijection between F-representations of G with degree n and right FG-modules of F-dimension n. For example, the right regular permutation representation arises from the group algebra FG itself, regarded as a right FG-module via right multiplication.

Convention. All modules are right modules unless the contrary is stated.

Equivalent Representations

Two F-representations ρ and σ of a group G are said to be *equivalent* if they arise from isomorphic FG-modules M and N. In particular, equivalent representations have the same degree.

Suppose that $\alpha: M \to N$ is an isomorphism of FG-modules, so that $(ag)\alpha = (a\alpha)g$ for all $a \in M$ and $g \in G$. Then, proceeding to the associated representations, we have $ag^\rho\alpha = a\alpha g^\sigma$; hence

$$\alpha^{-1}g^\rho\alpha = g^\sigma, \qquad (g \in G).$$

In terms of matrices this means that ρ^* and σ^* represent G by conjugate subgroups of $\mathrm{GL}(n, F)$. Naturally we shall be interested in representations only up to equivalence.

Reducible and Irreducible Representations

An F-representation ρ of G is called *reducible* if the associated FG-module M has a proper nonzero submodule. If, on the other hand, M has no proper nonzero submodules and is itself nontrivial—recall that such modules are said to be *simple*—then ρ is called an *irreducible representation.*

The simple FG-modules, and hence the irreducible F-representations of G, can be obtained from the group algebra in a very simple manner.

8.1.1. *If F is a field and G a group, a simple FG-module is FG-isomorphic with some FG/R where R is a maximal right ideal of FG.*

Proof. Let M be a simple FG-module and choose $a \neq 0$ in M. Then $r \mapsto ar$ is an FG-homomorphism from FG to M with nonzero image. Since M is simple, it must coincide with this image and $M \simeq_{FG} FG/R$ where R is the kernel. Finally R is clearly a maximal right ideal since M is simple. □

Of course, conversely, any such FG/R is a simple FG-module. Thus 8.1.1 suggests that knowledge of the structure of FG will aid us in determining the irreducible F-representations of G.

Direct Sums of Representations

Suppose that $M = M_1 \oplus \cdots \oplus M_k$ is direct decomposition of an FG-module M into submodules, and assume that M has finite F-dimension. Let ρ and ρ_i be the F-representations of G afforded by the modules M and M_i respectively. Then it is natural to say that ρ is the *direct sum of the representations* ρ_i and to write

$$\rho = \rho_1 \oplus \cdots \oplus \rho_k.$$

If we choose an F-basis for each M_i and take the union of these in the natural order to form a basis of M, the matrix representations ρ^* and ρ_i^* are related by the equation

$$x^{\rho^*} = \begin{bmatrix} x^{\rho_1^*} & & & 0 \\ & x^{\rho_2^*} & & \\ & 0 & \ddots & \\ & & & x^{\rho_k^*} \end{bmatrix}.$$

Completely Reducible Representations

We recall (from 3.3) that a module is completely reducible if it is a direct sum of simple modules. Accordingly an F-representation of a group G shall be called *completely reducible* if it arises from a completely reducible FG-module. Thus a completely reducible representation is a direct sum of (finitely many) irreducible representations and may be considered known if its irreducible components are known. Our attention is therefore directed at two problems: (i) determine which representations are completely reducible; (ii) determine all irreducible representations. We take up the first question next.

Criteria for Complete Reducibility

By far and away the most important condition for complete reducibility is *Maschke's Theorem.*

8.1.2 (Maschke). *Let G be a finite group and let F be a field whose characteristic does not divide the order of G. Then every F-representation of G is completely reducible.*

Proof. Let M be an FG-module of finite F-dimension. By 3.3.13 we need only prove that an FG-submodule N is a direct summand of M.

Since M is a vector space, we can certainly write $M = N \oplus L$ where L is an F-subspace (but perhaps not an FG-submodule). Let π be the canonical projection from M to N; this is certainly an F-homomorphism. To construct an FG-homomorphism we employ an averaging process: define π^* to be the endomorphism of M given by

$$a\pi^* = \frac{1}{m} \sum_{x \in G} (ax)\pi \cdot x^{-1}$$

where $m = |G|$. Note that this exists since m is finite and indivisible by the characteristic of F.

Clearly π^* is an F-endomorphism: in fact π^* is an FG-endomorphism because if $a \in M$ and $g \in G$,

$$\begin{aligned}(ag)\pi^* \cdot g^{-1} &= \frac{1}{m} \sum_{x \in G} (agx)\pi \cdot x^{-1}g^{-1} \\ &= \frac{1}{m} \sum_{y \in G} (ay)\pi \cdot y^{-1} = (a)\pi^*.\end{aligned}$$

Now $M\pi^* \leq N$ since $M\pi = N$ and N is a submodule. Also, if $a \in N$, we have $(ax)\pi = ax$ and so $a\pi^* = a$ by definition of π^*. Thus $M\pi^* = N$ and $\pi^* = (\pi^*)^2$. Hence π^* is a projection and $M = N \oplus \operatorname{Ker} \pi^*$. □

The hypothesis that the characteristic of F does not divide $|G|$, which includes the case where F has zero characteristic, will be frequently encountered here. We shall not deal with the more difficult *modular representation theory*, which is concerned with representations over a field F whose characteristic divides $|G|$: this is largely the creation of R. Brauer. For an account of this theory we refer to [b17] or [b20].

Clifford's Theorem

There is another criterion for complete reducibility which has the advantage of making no restrictions on field or group.

8.1.3 (Clifford). *Let G be any group, F any field and M a simple FG-module with finite F-dimension. Let H be a normal subgroup of G.*

(i) *If S is a simple FH-submodule of M, then $M = \sum_{g \in G} Sg$ and each Sg is a simple FH-module. Thus M is a completely reducible FH-module.*
(ii) *Let $S_1, \ldots, S_k$ be representatives of the isomorphism types of simple FH-submodules of M. Define M_i to be the sum of all FH-submodules of M that are isomorphic with S_i. Then $M = M_1 \oplus \cdots \oplus M_k$ and M_i is a direct sum of FH-modules isomorphic with S_i.*

(iii) *The group G permutes the "homogeneous components" M_i transitively by means of the right action on M.*
(iv) *If K_i is the subgroup of all g in G such that $M_i g = M_i$, then M_i is a simple FK_i-module.*

Proof. (i) Obviously $\sum_{g \in G} Sg$ is an FG-submodule, so it equals M by simplicity of the latter module. Now $(ag)h = (ah^{g^{-1}})g$ and $h^{g^{-1}} \in H$ if $h \in H$ and $g \in G$. Hence Sg is an FH-submodule. Moreover the mapping $a \mapsto ag$ is an F-isomorphism which maps FH-submodules onto FH-submodules, so Sg is simple. By 3.3.11 the FH-module M is completely reducible.

(ii) First of all observe that there are only finitely many isomorphism types: for M, having finite F-dimension, satisfies both chain conditions on FH-submodules and thus the Jordan–Hölder Theorem (3.1.4) applies. Since M is completely reducible, $M = M_1 + \cdots + M_k$. Also M_i is a direct sum of FH-modules isomorphic with S_i. If $M_i \cap \sum_{j \neq i} M_j \neq 0$, this intersection would contain a simple FH-submodule which, by the Jordan–Hölder Theorem, would be isomorphic with S_i and also with some S_j, $j \neq i$. This is impossible, so $M = M_1 \oplus \cdots \oplus M_k$.

(iii) If U is a simple FH-submodule of M_i and $g \in G$, then $Ug \overset{FH}{\simeq} S_j$ for some j, by (i): hence $M_i g \leq M_j$. Also $M_j g^{-1} \leq M_i$, so that $M_i g = M_j$. Thus G does indeed permute the M_i. Since the sum of the M_i in a G-orbit is an FG-module, G permutes the M_i transitively.

(iv) Let $\{t_1, \ldots, t_k\}$ be a right transversal to K_1 in G. Then $M_i = M_1 t_i$ for $i = 1, \ldots, k$, after the t_i have been suitably labeled: thus $M = M_1 t_1 \oplus \cdots \oplus M_1 t_k$. Suppose that N_1 is a proper nonzero FK_1-submodule of M_1 and write $N = \sum_{i=1}^{k} N_1 t_i$. Now $t_i g = h t_j$ for some $h \in K_1$ and j; therefore $(N_1 t_i)g = (N_1 h)t_j = N_1 t_j$. Consequently N is an FG-module and $M = N$. But $N_1 t_i \leq M_1 t_i = M_i$, so that $N_1 = M_1$, a contradiction. Hence M_1 is a simple FK_1-module; this implies that $M_i = M_1 t_i$ is a simple FK_i-module because $K_i = K_1^{t_i}$. □

Schur's Lemma and Applications

The following result is traditionally known as Schur's Lemma. Despite its simplicity, it is enormously useful.

8.1.4. *Let M and N be simple modules over a ring R. If M and N are not isomorphic,* $\operatorname{Hom}_R(M, N) = 0$. *Also* $\operatorname{Hom}_R(M, M) \equiv \operatorname{End}_R(M)$ *is a division ring.*

Proof. Let $\alpha: M \to N$ be an R-homomorphism. Then $\operatorname{Ker} \alpha$ and $\operatorname{Im} \alpha$ are submodules of M and N respectively. Since M and N are simple, either $\alpha = 0$ or $\operatorname{Ker} \alpha = 0$ and $\operatorname{Im} \alpha = N$; in the latter event α is an isomorphism. Hence $\operatorname{Hom}_R(M, N) = 0$ if M and N are not isomorphic, and each nonzero element of $\operatorname{End}_R(M)$ has an inverse. □

Probably the most useful form of 8.1.4 is the following special case.

8.1.5. *Let F be an algebraically closed field, A an F-algebra, and M a simple A-module with finite F-dimension. Then* $\mathrm{End}_A(M)$ *consists of all scalar multiplications by elements of F and* $\mathrm{End}_A(M) \simeq F$.

Proof. If $\alpha \in \mathrm{End}_A(M)$, then α is a linear transformation of the finite dimensional vector space M, and, because F is algebraically closed, α has a characteristic root in F, say f; thus $m\alpha = fm$ for some nonzero m in M. Now define $S = \{x \in M \mid x\alpha = fx\}$ and observe that S is a nonzero F-subspace of M. If $m \in S$ and $a \in A$, we have $(ma)\alpha = (m\alpha)a = f(ma)$, so that S is an A-submodule. By simplicity of M we have $S = M$, which shows that $m\alpha = fm$ for all m in M, and α is scalar. □

This result has immediate application to irreducible representations of abelian groups over algebraically closed fields.

8.1.6. *An irreducible representation of an abelian group G over an algebraically closed field F has degree* 1.

Proof. Let M be a simple FG-module with finite F-dimension. Applying 8.1.5 with $A = FG$, we conclude that $\mathrm{End}_{FG}(M)$ consists of scalar multiplications. But for any g in G the mapping $a \mapsto ag$ is an FG-endomorphism of M because G is abelian. This mapping is therefore scalar and $ag = f_g a$ for some f_g in F. Consequently every one-dimensional subspace is a submodule and M has dimension 1. □

A Theorem of Burnside

We aim next to prove an important theorem of Burnside on irreducible representations over algebraically closed fields. In addition to Schur's Lemma we shall need the following result.

8.1.7 (The Jacobson Density Theorem). *Let R be a ring with identity and let M be a simple R-module. Write $S = \mathrm{End}_R(M)$ and choose α from* $\mathrm{End}_S(M)$. *Then to each finite subset $\{a_1, \dots, a_m\}$ of M there corresponds an element r of R such that $a_i\alpha = a_i r$ for $i = 1, 2, \dots, m$.*

Proof. Form a direct sum L of m copies of M and define $\alpha^*\colon L \to L$ by the rule $(x_1, \dots, x_m)\alpha^* = (x_1\alpha, \dots, x_m\alpha)$. Clearly α^* is an endomorphism of L and in fact $\alpha^* \in \mathrm{End}_T(L)$ where $T = \mathrm{End}_R(L)$. To see this let $\tau \in T$ and write $(x_1, 0, \dots, 0)\tau = ((x_1)\tau_{11}, (x_1)\tau_{12}, \dots, (x_1)\tau_{1m})$ where $(x_1)\tau_{1j} \in M$: now $\tau_{1j} \in \mathrm{End}_R(M)$ since $\tau \in \mathrm{End}_R(L)$. Therefore, since $\alpha \in \mathrm{End}_S(M)$,

$$\begin{aligned}(x_1, 0, \dots, 0)\tau\alpha^* &= ((x_1)\tau_{11}\alpha, \dots, (x_1)\tau_{1m}\alpha) \\ &= ((x_1)\alpha\tau_{11}, \dots, (x_1)\alpha\tau_{1m}) = (x_1, 0, \dots,)\alpha^*\tau.\end{aligned}$$

Similarly $\tau\alpha^*$ and $\alpha^*\tau$ agree on $(0, x_2, 0, \ldots, 0)$, etc. Thus $\tau\alpha^* = \alpha^*\tau$ and $\alpha^* \in \mathrm{End}_T(M)$.

Now L is visibly completely reducible; thus, on writing $a = (a_1, \ldots, a_m)$, we have $L = aR \oplus N$ for some R-submodule N by 3.3.12. Let π be the canonical projection from L to aR. Then $\pi \in T$. Since R has an identity element, $a \in aR$; therefore $a = a\pi$ and $a\alpha^* = (a\pi)\alpha^* = (a\alpha^*)\pi \in aR$. It follows that $a\alpha^* = ar$ for some r in R, and $a_i\alpha = a_ir$ for $i = 1, 2, \ldots, m$. □

8.1.8 (Burnside). *Let ρ be an irreducible representation of a group G with degree n over an algebraically closed field F. Let M be the associated FG-module. Then the set $\{g^\rho | g \in G\}$ generates* $\mathrm{End}_F(M)$ *as a vector space and therefore contains n^2 linearly independent elements.*

Proof. Let $R = FG$. By Schur's Lemma $S = \mathrm{End}_R(M)$ consists of all scalar multiplications and therefore $\mathrm{End}_S(M) = \mathrm{End}_F(M)$. It follows from 8.1.7 that every linear transformation of M arises from right multiplication by an element of R and is therefore a linear combination of g^ρ's. Consequently the g^ρ's generate $\mathrm{End}_F(M)$. Since the latter has F-dimension n^2, the second part follows. □

There are some interesting applications of Burnside's theorem to groups of matrices. If G is a subgroup of $\mathrm{GL}(n, F)$, then of course the inclusion $G \hookrightarrow \mathrm{GL}(n, F)$ is a matrix representation of G over F, and G may be called reducible, irreducible etc. according as this representation has the property stated. Moreover, if V is a vector space of dimension n over F, on choosing a basis of V we obtain an action of G on V making the latter an FG-module.

We proceed to derive a basic lemma.

8.1.9. *Let G be an irreducible subgroup of* $\mathrm{GL}(n, F)$ *where F is an algebraically closed field. Suppose that the set* $\{\mathrm{trace}(g) | g \in G\}$ *has a finite number of elements, say m. Then G is finite and $|G| \leq m^{n^2}$.*

Proof. Apply 8.1.8 with ρ the inclusion $G \hookrightarrow \mathrm{GL}(n, F)$; then there are n^2 linearly independent elements of G, say $g_1, \ldots, g_{n^2}$. Choose any g in G and write $g(i, j)$ for the (i, j) entry of the $n \times n$ matrix g. Denoting $\mathrm{trace}(g_ig)$ by t_i, we obtain equations

$$\sum_{j,k=1}^{n} g_i(j, k)\cdot g(k, j) = t_i, \qquad i = 1, 2, \ldots, n^2.$$

These constitute a linear system in the n^2 unknowns $g(k, j)$. Because $g_1, \ldots, g_{n^2}$ are linearly independent, there is a unique solution of this system, by a basic theorem of linear algebra. This solution determines g completely. Since $t_1, \ldots, t_{n^2}$ can be selected in at most m^{n^2} ways, we conclude that $|G| \leq m^{n^2}$. □

Our first application involves *unipotent matrices*. An element g of $GL(n, F)$ is termed *unipotent* if $(g - 1)^m = 0$ for some $m > 0$. It is an easy exercise to verify that g is unipotent if and only if all its characteristic roots equal 1. Clearly every unitriangular matrix is unipotent. The following is a partial converse of this statement.

8.1.10. *Let G be a subgroup of* $GL(n, F)$ *where F is any field. If every element of G is unipotent, then G is conjugate to a subgroup of $U(n, F)$, the group of all upper unitriangular matrices.*

Proof. Let G act on a vector space V of dimension n. It is enough to prove that there is a series of FG-submodules $0 = V_1 \leq V_1 \leq \cdots \leq V_k = V$ such that G operates trivially on V_{i+1}/V_i. For then, on choosing suitable bases for the V_i, we can represent the elements of G by unitriangular matrices.

Suppose first that F is algebraically closed. We may assume that G is irreducible, otherwise induction on n yields the result. By hypothesis the trace of every element of G equals n, so 8.1.9 may be applied to give $|G| = 1$.

Now suppose that F is not necessarily algebraically closed and write $\bar{F}$ for its algebraic closure. Let $\bar{V} = \bar{F} \otimes_F V$ and view this as an $\bar{F}G$-module. By the last paragraph there is a series of $\bar{F}G$-modules $0 = \bar{V}_0 \leq \bar{V}_1 \leq \cdots \leq \bar{V}_k = \bar{V}$ with $\bar{V}_{i+1}/\bar{V}_i$ a trivial module. We can identify a in V with $1 \otimes a$ in $\bar{V}$, so that $V \leq \bar{V}$, and define $V_i = V \cap \bar{V}_i$. Then the V_i form a series of the required type. □

Our second application is to matrix groups that are torsion groups.

8.1.11

(i) (Burnside). *If F is a field of characteristic* 0, *a subgroup of* $GL(n, F)$ *with finite exponent is finite.*
(ii) (Schur). *A torsion subgroup of* $GL(n, \mathbb{Q})$ *is finite.*

Proof. It is evident that we can assume F to be algebraically closed in (i). We suppose first that G is irreducible. If G has exponent e and $g \in G$, then $g^e = 1$, whence each characteristic root of g is an eth root of unity in F. Since F contains at most e such roots, there are no more than e^n values of trace (g). By 8.1.9 the group G is finite. Now assume that G is reducible, If G acts on a vector space V of dimension n, there is a proper nonzero FG-submodule U. By 1.3.12 and induction on n, if L is the subgroup of elements of G which act trivially on U and on V/U, then $|G : L|$ is finite. But L is isomorphic with a group of unitriangular matrices over F, whence it is torsion-free since F has characteristic zero. Hence $L = 1$ and G is finite.

To establish (ii) it suffices to prove that G has finite exponent since (i) may then be applied. Let g in G have order m and put $H = \langle g \rangle$. It will be shown that the integer m can be bounded in terms of n. By induction we can assume that H is irreducible.

By Schur's Lemma $\mathrm{End}_H(V)$ is a division algebra over $\mathbb{Q}$ and its center is a field E containing $\mathbb{Q}$. Clearly $g \in E$. Since the cyclotomic polynomial Φ_m is irreducible, it is the irreducible polynomial of g over $\mathbb{Q}$: let $l = \deg \Phi_m = \varphi(m)$. If $0 \neq u \in V$, then $u, ug, \ldots, ug^{l-1}$ are linearly independent; otherwise the degree of the irreducible polynomial of g would be less than l. Hence $l \leq \dim V = n$, so that m is bounded by a function of n. □

EXERCISES 8.1

1. Prove that Maschke's Theorem does not hold if: (i) the characteristic of the field divides the order of the group; or (ii) the group is infinite.

*2. A permutation representation of degree > 1 is reducible.

3. Let G be a (possibly infinite) group and let H be a subgroup with finite index. Suppose that F is a field whose characteristic does not divide $|G:H|$ and that M is an FG-module which is completely reducible as an FH-module. Prove that M is completely reducible as an FG-module. [*Hint*: Imitate the proof of Maschke's Theorem.]

*4. Let G be a finite group which has a unique minimal normal subgroup and let F be a field whose characteristic does not divide $|G|$. Prove that G has a faithful irreducible F-representation. [*Hint*: Apply 8.1.2 to FG.]

5. An irreducible representation of a finite p-group over a field with characteristic p has degree 1.

6. Prove that a cyclic group of order n has a faithful irreducible $\mathbb{Q}$-representation of degree $\varphi(n)$ (where φ is Euler's function).

7. A matrix over a field is unipotent if and only if all its characteristic roots equal 1.

8. If G is a subgroup of $\mathrm{GL}(n, F)$, $n > 1$, and $(g - 1)^{r(g)} = 0$ for some $r(g) > 0$ and all $g \in G$, then G is nilpotent of class at most $n - 1$.

9. If F is a field of characteristic 0, a subgroup of $\mathrm{GL}(n, F)$ with finite exponent e has order at most e^{n^3}.

10. There is an upper bound depending only on n for the order of a finite subgroup of $\mathrm{GL}(n, \mathbb{Q})$.

11. A finite p-group G has a faithful irreducible representation over an algebraically closed field whose characteristic is not p if and only if the centre of G is cyclic.

12. Let n be the degree of an irreducible representation of a finite group G over an algebraically closed field. Prove that $n^2 \leq |G : \zeta G|$. [*Hint*: Apply 8.1.8.]

13. (Burnside) Prove that a subgroup of $\mathrm{GL}(n, F)$ with finite class number is finite for any field F. [*Hint*: Use induction on n and 8.1.9.]

8.2. Structure of the Group Algebra

We shall now investigate the structure of the group algebra using Maschke's Theorem and Schur's Lemma.

8.2.1. *If G is a finite group and F is a field whose characteristic does not divide the order of G, then FG has no nonzero nilpotent right ideals.*

Proof. Let S be a nilpotent right ideal of $R = FG$. By Maschke's Theorem R is completely reducible as a right R-module. Hence $R = S \oplus T$ for some right ideal T, and we can write $1 = s + t$ where $s \in S$ and $t \in T$. Right multiplication by s yields $ts = s - s^2 \in S \cap T = 0$. Hence $s = s^2$, which implies that $s = 0$ because S is nilpotent. Thus $t = 1$, so that $T \geq 1R = R$ and $S = 0$. □

Definition. If R and S are rings, an *anti-homomorphism* from R to S is a homomorphism $\alpha: R \to S$ of additive groups such that

$$(r_1 r_2)\alpha = (r_2\alpha)(r_1\alpha), \qquad (r_i \in R).$$

An anti-homomorphism which is bijective is called an *anti-isomorphism.*

The next result is very simple.

8.2.2. *Let R be any ring with an identity element and let R_R denote the ring R when regarded as a right R-module in the natural way. If $r \in R$, define $r': R_R \to R_R$ by $xr' = rx$. Then $r \mapsto r'$ is an anti-isomorphism from R to $\text{End}_R(R_R)$.*

Proof. In the first place r' is certainly an endomorphism of the underlying additive group of R: also $(xr_1)r' = rxr_1 = ((x)r')r_1$, so in fact $r' \in E = \text{End}_R(R_R)$. It is equally easy to see that $(r_1 + r_2)' = r_1' + r_2'$ and $(r_1 r_2)' = r_2' r_1'$, so that the mapping $r \mapsto r'$ is an anti-homomorphism: let us call it θ. If $r' = 0$, then $0 = (1)r' = r$, so θ is injective. Finally let $\xi \in E$ and put $s = (1)\xi$; then $r\xi = (1r)\xi = (1)\xi r = sr = rs'$ for all $r \in R$. Thus $\xi = s'$ and θ is also surjective. □

We precede the main structure theorem for group algebras with a remark about endomorphism rings. Let $M = M_1 \oplus \cdots \oplus M_k$ be a direct decomposition of an R-module M into R-submodules. Let $\xi \in \text{End}_R(M)$ and, if $a \in M_i$, define $a\xi_{ij}$ to be the M_j-component of $a\xi$. Then $\xi_{ij} \in \text{Hom}_R(M_i, M_j)$. Thus we can associate with ξ the $k \times k$ matrix ξ^* whose (i, j) entry is ξ_{ij}. It is easy to verify that $\xi \mapsto \xi^*$ is a ring isomorphism from $\text{End}_R(M)$ to the ring of all $k \times k$ matrices with (i, j) entries in $\text{Hom}_R(M_i, M_j)$, the addition and multiplication rules being the usual ones for matrices.

8.2.3. *Let G be a finite group and let F be an algebraically closed field whose characteristic does not divide the order of G.*

(i) $FG = I_1 \oplus I_2 \oplus \cdots \oplus I_h$ *where I_i is an ideal of FG which is ring isomorphic with the ring $M(n_i, F)$ of all $n_i \times n_i$ matrices over F.*
(ii) $|G| = n_1^2 + n_2^2 + \cdots + n_h^2$.
(iii) *Each simple FG-module is isomorphic with a minimal right ideal of some I_i and has F-dimension n_i. Thus the n_i are the degrees of the irreducible F-representations of G.*
(iv) *The number h of inequivalent irreducible F-representations of G equals the class number of G.*

Proof. Let $R = FG$. By Maschke's Theorem R is a direct sum of minimal right ideals. Just as in the proof of 8.1.3 we can group isomorphic minimal right ideals of R together to form "homogeneous components" I_i. Then $R_R = I_1 \oplus \cdots \oplus I_h$ where I_i is the sum of all minimal right ideals isomorphic with a given one, say S_i. If $r \in R$, then $s \mapsto rs$ is an R-epimorphism from S_i to rS_i, whence either $rS_i = 0$ or $rS_i \simeq S_i$. From this is follows that $rI_i \leq I_i$, which shows I_i to be an ideal of R.

Next consider $E = \text{End}_R(R_R)$. In view of the decomposition $R_R = I_1 \oplus \cdots \oplus I_h$ and the remarks immediately preceding this proof, we may represent ξ in E by an $h \times h$ matrix $\xi^* = (\xi_{ij})$ where $\xi_{ij} \in \text{Hom}_R(I_i, I_j)$. If $i \neq j$, then $\text{Hom}_R(S_i, S_j) = 0$ by Schur's Lemma, which clearly implies that $\text{Hom}_R(I_i, I_j) = 0$. Thus ξ^* is diagonal and $\xi \mapsto \xi^*$ yields a ring isomorphism

$$E \simeq \text{End}_R I_1 \oplus \cdots \oplus \text{End}_R I_h.$$

Now by 8.1.5 we have $\text{End}_R(S_i) \simeq F$ and thus $\text{End}_R(I_i) \simeq M(n_i, F)$, where n_i is the number of simple summands in the direct decomposition of I_i.

From 8.2.2 we obtain an anti-isomorphism from R to E; we also have an isomorphism from E to $M(n_1, F) \oplus \cdots \oplus M(n_h, F) = M$ and finally an anti-isomorphism from M to M generated by transposing matrices. Composition of these three functions yields an isomorphism from R to M. Thus (i) is established.

The F-dimension of R is certainly $|G|$, while that of $M(n_i, F)$ is n_i^2. Taking F-dimensions of both sides in (i), we obtain $|G| = n_1^2 + \cdots + n_h^2$, thus proving (ii).

By 8.1.1 a simple R-module is an image of R and thus, by 8.1.2, is R-isomorphic with some minimal right ideal of R contained in one of the M_i. If X is a right ideal of I_i, it is also a right ideal of R: for $XI_j \leq I_i \cap I_j = 0$ if $j \neq i$, and hence $XR \leq X$. Therefore $X \subseteq I_i$ is a minimal right ideal of R if and only if it is a minimal right ideal of I_i. By (i) we need to show that some minimal right ideal of the matrix ring $M(n, F)$ has dimension n over F.

Let E_{ij} denote the $n \times n$ elementary matrix whose (i, j) entry is 1 and whose other entries are 0. Define $J_i = FE_{i1} + \cdots + FE_{in}$: obviously J_i is a right ideal of $M(n, F)$. Suppose that $0 < T \leq J_i$ where T is a right ideal of

$M(n, F)$, and let $0 \neq t = \sum_j f_j E_{ij} \in T$. If, say, $f_k \neq 0$, then

$$E_{im} = t(f_k^{-1} E_{km}) \in T$$

for all m, which proves that $T = J_i$ and J_i is a minimal right ideal of $M(n, F)$. The F-dimension of J_i is n.

It remains only to show that h equals the class number l of G. To achieve this we consider the *center* C of the ring R, which is defined to be the subset of elements r such that $rx = xr$ for all x in R. Clearly C is a subring of R. Now C is evidently the sum of the centres of the I_i. Also the center of $M(n, F)$ is well-known to consist of the scalar matrices; hence its dimension is 1. It follows that C has F-dimension h.

Denote the conjugacy classes of G by $K_1, \dots, K_l$ and define $k_i = \sum_{x \in K_i} x$. Clearly $g^{-1} k_i g = k_i$, so that $k_i g = g k_i$ for all g in G; thus $k_i \in C$. Moreover $k_1, \dots, k_l$ are linearly independent over F, so $l \leq h$. If we can show that $C = Fk_1 + \cdots + Fk_l$, it will follow that $h = l$. Suppose that $c = \sum_{x \in G} f_x x \in C$. Then for all g in G

$$c = g^{-1}\left(\sum_{x \in G} f_x x\right) g = \sum_{x \in G} f_x (g^{-1} x g) = \sum_{y \in G} f_{gyg^{-1}} y.$$

Hence $f_y = f_{gyg^{-1}}$, which shows that f is constant on K_i: let its value be f_i. Then $c = \sum_{i=1}^{l} f_i k_i$, and we are finished. □

Example. Consider $\mathbb{C}G$ where $G = S_3$, the symmetric group of degree 3, and $\mathbb{C}$ is the complex field. Since G has three conjugacy classes, there are three inequivalent irreducible representations of G over $\mathbb{C}$, with degrees n_1, n_2, n_3 satisfying $n_1^2 + n_2^2 + n_3^2 = 6$; this has the solution $n_1 = 1 = n_2$, $n_3 = 2$. Hence $\mathbb{C}G \simeq \mathbb{C} \oplus \mathbb{C} \oplus M(2, \mathbb{C})$.

In this case it is easy to identify the irreducible representations. Let $G = \langle x, y \rangle$ where $x = (1, 2, 3)$ and $y = (1, 2)(3)$. The two irreducible representations of degree 1 are the trivial representation and the representation $g \mapsto \operatorname{sign} g$. The representation of degree 2 may be described by the assignments

$$x \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Clearly this is a faithful representation.

Exercises 8.2

1. Let G be a finite group and F any field whose characteristic does not divide $|G|$. Prove that the number of inequivalent irreducible F-representations of G cannot exceed the class number of G, and give an example to show that it may be smaller than the class number.

2. Let G be a cyclic group of finite order n. Determine all the irreducible $\mathbb{C}$-representations and all the irreducible $\mathbb{Q}$-representations of G. For which n are their numbers equal? Also describe the structure of $\mathbb{C}G$ and $\mathbb{Q}G$.

3. Find all the inequivalent irreducible $\mathbb{C}$-representations of A_4. Describe the structure of the group algebra $\mathbb{C}(A_4)$.
4. Repeat Problem 3 for D_8.
5. How many inequivalent irreducible $\mathbb{C}$-representations does S_n have? In the case of S_4 find the degrees of these representations.
6. Let G be a finite p-group and let F be a field of characteristic p. Define I to be the F-subspace of $R = FG$ generated by all $g - 1$, $g \in G$.
   (a) Prove that I is an ideal of R and $R/I \simeq F$.
   (b) Show that I is nilpotent and coincides with the sum of all nilpotent right ideals of R.
   (c) A simple FG-module is isomorphic with the trivial module F. Find a submodule of R that gives rise to the trivial representation.

8.3. Characters

Let ρ be an F-representation of a group G and suppose that ρ arises from an FG-module M. If we choose an F-basis for M, there is a corresponding matrix representation ρ^*. Choice of another basis for M would lead to a matrix similar to x^{ρ^*} representing x. Now similar matrices have the same trace. Hence the function

$$\chi\colon G \to F$$

defined by

$$(x)\chi = \text{trace}(x^{\rho^*})$$

is independent of the choice of basis. We call χ the *character* of the representation ρ or the module M. The character χ is said to be *irreducible*, *faithful*, etc. if the associated representation ρ has the property in question.

The fundamental property of characters is that they are class functions. Here a *class function* from G to F is a function $\alpha\colon G \to F$ such that $(g^{-1}xg)\alpha = (x)\alpha$: in words, α is constant on each conjugacy class of G.

8.3.1. *Characters are class functions.*

Proof. Let χ be the character of an F-representation ρ of G. Then $(g^{-1}xg)^{\rho^*} = (g^{\rho^*})^{-1}\chi^{\rho^*}g^{\rho^*}$ where ρ^* is an associated matrix representation. Thus $(g^{-1}xg)\chi = \text{trace}((g^{\rho^*})^{-1}x^{\rho^*}g^{\rho^*}) = \text{trace } x^{\rho^*} = (x)\chi$. □

If ρ and σ are equivalent F-representations of G, then G^{ρ^*} and G^{σ^*} are conjugate in $\text{GL}(n, F)$. Using again the fact that similar matrices have the same trace one has the following fact.

8.3.2. *Equivalent representations have the same character.*

That it is the *irreducible* characters which are of interest is made plain by the next result. Here the *sum* $\chi + \psi$ of characters χ and ψ is defined by the rule $(x)\chi + \psi = (x)\chi + (x)\psi$.

8.3.3. *Every character is a sum of irreducible characters.*

Proof. Let M be an FG-module with finite dimension over F affording a representation ρ. Let $0 = M_0 < M_1 < \cdots < M_r = M$ be an FG-composition series of M. Write χ for the character of M and χ_i for the character of the simple module M_i/M_{i-1}. Choose a basis for M_1, extend it to basis of M_2, then to a basis of M_3, and so on. This results in a basis of M with respect to which the associated matrix representation is given by

$$x^{\rho^*} = \begin{bmatrix} x^{\rho_1^*} & & & 0 \\ & x^{\rho_2^*} & & \\ & * & \ddots & \\ & & & x^{\rho_r^*} \end{bmatrix};$$

here ρ_i is the representation afforded by M_i/M_{i-1}. Taking the trace of the matrix x^{ρ^*}, we obtain $(x)\chi = (x)\chi_1 + \cdots + (x)\chi_r$ and $\chi = \chi_1 + \cdots + \chi_r$. □

Orthogonality Relations

Let G be a finite group and let F be any field. Consider the set

$$S(G, F)$$

of all functions from G to F. The rules

$$(x)\alpha + \beta = (x)\alpha + (x)\beta \qquad \text{and} \qquad (x)a\alpha = a(x\alpha)$$

where $x \in G$, $a \in F$ and $\alpha, \beta \in S(G, F)$, make $S(G, F)$ into a vector space over F. If δ_g denotes the function which maps g to 1_F and all other elements of G to 0_F, then the δ_g are obviously linearly independent in $S(G, F)$. Also, for any α in $S(G, F)$ we have $\alpha = \sum_{x \in G} (x)\alpha \cdot \delta_x$, by direct comparison of the values of the two functions. Hence the set $\{\delta_g | g \in G\}$ is a basis for $S(G, F)$ and the latter has dimension $|G|$. It is also easy to verify that *the class functions from G to F form a subspace of $S(G, F)$ with dimension equal to the class number of G.*

Select an F-representation ρ of G and let M be an FG-module which gives rise to ρ. Choosing a basis for M, we write $(x)\rho_{ij}$ for the (i, j) entry of the matrix x^{ρ^*} where as usual ρ^* is the corresponding matrix representation. Thus associated with ρ are the n^2 functions ρ_{ij}: $G \to F$ in $S(G, F)$.

The following result is basic.

8.3.4. *Let G be a finite group, F a field, and ρ, σ irreducible F-representations of G. Let ρ_{ij}, σ_{ij} denote the associated matrix functions (with respect to fixed bases).*

(i) *If ρ and σ are inequivalent, then $\sum_{x\in G}(x)\rho_{ij}(x^{-1})\sigma_{rs} = 0$.*
(ii) *If F is algebraically closed and its characteristic does not divide $|G|$, then*

$$\sum_{x\in G}(x)\rho_{ij}(x^{-1})\rho_{rs} = \frac{|G|}{n}\delta_{is}\delta_{jr}$$

where n is the degree of ρ and δ_{uv} is the "Kronecker delta."

Proof. Let ρ and σ arise from FG-modules M and N. For any η in $\mathrm{Hom}_F(M, N)$ define $\bar{\eta}$ in $\mathrm{Hom}_F(M, N)$ by

$$\bar{\eta} = \sum_{x\in G} x^{\rho}\eta(x^{-1})^{\sigma}. \tag{1}$$

If $g \in G$, then

$$\bar{\eta}g^{\sigma} = \sum_{x\in G} x^{\rho}\eta(x^{-1}g)^{\sigma} = \sum_{\eta\in G}(gy)^{\rho}\eta(y^{-1})^{\sigma} = g^{\rho}\bar{\eta},$$

which shows that $\bar{\eta} \in \mathrm{Hom}_{FG}(M, N)$.

Now choose η to be the linear transformation which maps the jth basis element of M to the rth basis element of N and all other basis elements of M to 0. Then η is represented by a matrix whose (k, l) entry is $\delta_{jk}\delta_{rl}$. Taking the matrix form of (1) we obtain

$$\bar{\eta}_{is} = \sum_{x\in G}\sum_{k}\sum_{l}(x)\rho_{ik}\delta_{jk}\delta_{rl}(x^{-1})\sigma_{ls} = \sum_{x\in G}(x)\rho_{ij}(x^{-1})\sigma_{rs}.$$

If ρ and σ are inequivalent, $\mathrm{Hom}_{FG}(M, N) = 0$ by Schur's Lemma, and $\bar{\eta} = 0$: thus (i) follows at once. To prove (ii) put $\sigma = \rho$, so that $\bar{\eta} \in \mathrm{End}_{FG}(M)$ and $\bar{\eta}$ is scalar by 8.1.5; thus $\bar{\eta} = f_{jr}1$ where $f_{jr} \in F$. Then the equation for $\bar{\eta}_{is}$ yields

$$f_{jr}\delta_{is} = \sum_{x\in G}(x)\rho_{ij}(x^{-1})\rho_{rs} = \sum_{y\in G}(y)\rho_{rs}(y^{-1})\rho_{ij} = f_{si}\delta_{rj}. \tag{2}$$

Therefore $\sum_x (x)\rho_{ij}\cdot(x^{-1})\rho_{rs} = 0$ if either $i \neq s$ or $j \neq r$. Furthermore (2) yields also $f_{jj} = \sum_x (x)\rho_{ij}\cdot(x^{-1})\rho_{ji} = f_{ii}$. Thus $f = f_{jj}$ is independent of j. Hence

$$\begin{aligned} nf = \sum_{j=1}^{n}\left(\sum_x (x)\rho_{ij}(x^{-1})\rho_{ji}\right) &= \sum_x\left(\sum_{j=1}^{n}(x)\rho_{ij}(x^{-1})\rho_{ji}\right) \\ &= \sum_x ((xx^{-1})\rho_{ii}) \\ &= |G|. \end{aligned}$$

Since $|G|$, and hence n, is not divisible by the characteristic of F, it follows that $f = |G|/n$. This completes the proof. □

From this result may be deduced the fundamental *orthogonality relations* which connect the irreducible characters.

8.3.5 (Frobenius). *Let G be a finite group and F a field. Let χ and ψ be distinct irreducible F-characters of G.*

(i) $\sum_{x\in G}(x)\chi(x^{-1})\psi = 0$.
(ii) *If F is algebraically closed and its characteristic does not divide $|G|$, then* $\sum_{x\in G}(x)\chi(x^{-1})\chi = |G|$.
(iii) *If F has characteristic* 0, *then* $(1/|G|)\sum_{x\in G}(x)\chi(x^{-1})\chi$ *is always a positive integer.*

Proof. Let ρ and σ be irreducible representations with characters χ and ψ respectively. Then ρ and σ are inequivalent by 8.3.2. Let ρ_{ij} and σ_{ij} be the associated matrix functions with respect to fixed bases. Then $\chi = \sum_i \rho_{ii}$ and $\psi = \sum_j \sigma_{jj}$. By 8.3.4

$$\sum_{x\in G}(x)\chi(x^{-1})\psi = \sum_i\sum_j\left(\sum_{x\in G}(x)\rho_{ii}(x^{-1})\sigma_{jj}\right) = 0.$$

Now assume that F is algebraically closed with characteristic not dividing $|G|$. If n is the degree of ρ, we obtain from 8.3.4.

$$\sum_{x\in G}(x)\chi(x^{-1})\chi = \sum_i\sum_j\left(\sum_{x\in G}(x)\rho_{ii}(x^{-1})\rho_{jj}\right)$$
$$= \sum_i\sum_j\frac{|G|}{n}\delta_{ij}^2 = |G|.$$

Thus (i) and (ii) are proven.

Finally, assume only that F has characteristic 0 and let $\psi_1, \ldots, \psi_r$ be the irreducible characters of G over the algebraic closure of F. By 8.3.3 we can write $\chi = \sum_{j=1}^r m_j\psi_j$ where m_j is a nonnegative integer. Then applying the results of (i) and (ii), we have

$$\sum_{x\in G}(x)\chi(x^{-1})\chi = \sum_j\sum_k m_jm_k\left(\sum_x (x)\psi_j(x^{-1})\psi_k\right)$$
$$= \left(\sum_j m_j^2\right)|G|,$$

which yields (iii). □

The Inner Product of Characters

Let G be a finite group and F a field whose characteristic does not divide $|G|$. If α and β belong to $S(G, F)$, we define an element $\langle\alpha, \beta\rangle_G$ of F by

$$\langle\alpha, \beta\rangle_G = \frac{1}{|G|}\sum_{x\in G}(x)\alpha(x^{-1})\beta.$$

Clearly $\langle\ \ \rangle_G$ is a symmetric F-bilinear form on $S(G, F)$. Also, if $\langle\alpha, \beta\rangle_G = 0$

for all β, we could choose $\beta = \delta_{x^{-1}}$ concluding that $(x)\alpha = 0$ for all x and $\alpha = 0$. Thus $\langle \quad \rangle_G$ is nondegenerate. Hence $\langle \quad \rangle_G$ is an inner product on the vector space $S(G, F)$.

8.3.6. *Let G be a finite group and let F be an algebraically closed field whose characteristic does not divide $|G|$. Then the set of distinct irreducible F-characters of G is an orthonormal basis for the vector space of all class functions from G to F with respect to the inner product $\langle \quad \rangle_G$.*

Proof. Let $\chi_1, \ldots, \chi_h$ be the distinct irreducible F-characters of G. By 8.3.5 and the definition of the inner product $\langle \chi_i, \chi_j \rangle_G = \delta_{ij}$, which shows that the χ_i form an orthonormal set. By 8.2.3 the integer h is the class number of G, and this equals the dimension of the vector space of all class functions. Hence the χ_i form a basis for this space. □

We shall use these ideas to prove that if F has characteristic 0, an F-representation is determined up to eqivalence by its character. To specify the representations, therefore, it is in principle enough to exhibit the characters.

8.3.7. *Let G be a finite group and let F be a field of characteristic* 0. *Then F-representations of G with the same character are equivalent.*

Proof. Let $\rho_1, \ldots, \rho_h$ be a complete set of inequivalent irreducible F-representations of G. Then by Maschke's Theorem any F-representation is equivalent to one of the form $\rho = t_1\rho_1 \oplus \cdots \oplus t_h\rho_h$ where the t_i are nonnegative integers and $t_i\rho_i$ means the direct sum of t_i copies of ρ_i. Denote the characters of ρ and ρ_i by χ and χ_i respectively. Then $\chi = t_1\chi_1 + \cdots + t_h\chi_h$. By 8.3.5 we have $\langle \chi, \chi_i \rangle = l_i t_i$ where $l_i = \langle \chi_i, \chi_i \rangle$, a positive integer. Bearing in mind that F has characteristic 0, we have $t_i = \langle \chi, \chi_i \rangle l_i^{-1}$. Thus the t_i, and hence ρ, are determined by χ. □

This result is false if F has positive characteristic (Exercise 8.3.6).

Algebraic Integers

In order to prove the next main result some simple facts about algebraic integers are needed.

In the first place, recall that an *algebraic number field F* is a finite field extension of the rational field $\mathbb{Q}$. An *algebraic integer* in F is an element which is the root of a monic polynomial with integral coefficients. It is a simple exercise to prove that f in F is an algebraic integer if and only if the subring generated by f and 1_F is finitely generated as an abelian group.

8.3.8. *The algebraic integers in an algebraic number field F form a subring.*

Proof. Let f_1 and f_2 be two algebraic integers in F. Then $f_1^n + l_{n-1}f_1^{n-1} + \cdots + l_1 f_1 + l_0 = 0$ for certain integers l_i and $f_1^n \in \langle 1, f_1, \ldots, f_1^{n-1}\rangle$: a similar statement holds for f_2. It follows easily that the ring generated by $1, f_1$, and f_2 can be finitely generated *as an abelian group*. Hence the subrings generated by 1 and $f_1 \pm f_2$ and by 1 and $f_1 f_2$ are also finitely generated abelian groups (by 4.2.8). Consequently $f_1 \pm f_2$ and $f_1 f_2$ are algebraic integers. □

8.3.9. *A rational number which is an algebraic integer is an integer.*

Proof. Let m/n be an algebraic integer where m and n are relatively prime integers. Then m/n is the root of some monic polynomial $t^r + l_{r-1}t^{r-1} + \cdots + l_1 t + l_0$ in $\mathbb{Z}[t]$, and consequently $m^r + l_{r-1}m^{r-1}n + \cdots + l_1 mn^{r-1} + l_0 n^r = 0$. But this implies that n divides m^r, and hence that $n = \pm 1$. □

We can now establish the fundamental theorem on the degrees of the irreducible representations. The principal step in the proof is the following lemma.

8.3.10. *Let G be a finite group and let F be an algebraically closed field of characteristic* 0. *Suppose that χ is an irreducible F-character of G with degree n. If the element g has l conjugates in G, then $l((g)\chi)/n$ is an algebraic integer.*

Proof. Let $K_1, \ldots, K_h$ denote the conjugacy classes of G and let $k_i = \sum_{x \in K_i} x$. We have already observed that $k_1, \ldots, k_h$ form an F-basis for C, the center of FG. Since $k_i k_j \in C$,

$$k_i k_j = \sum_{r=1}^{h} m_{ij}^{(r)} k_r, \tag{3}$$

where $m_{ij}^{(r)}$ is the number of pairs (x, y) such that $x \in K_i$, $y \in K_j$, and xy equals a fixed element z_r in K_r. (Notice that $m_{ij}^{(r)}$ does not depend on the choice of z_r in K_r.)

Let $\rho\colon G \to \mathrm{GL}(M)$ be a representation with character χ. In the obvious way extend ρ and χ to FG. Then $k_i^\rho \in \mathrm{End}_{FG}(M)$, so that $k_i^\rho = f_i 1$ for some f_i in F by 8.1.5. Now $nf_i = \mathrm{trace}(k_i^\rho) = (k_i)\chi = l_i \chi^{(i)}$ where $l_i = |K_i|$ and $\chi^{(i)}$ is the value of χ on K_i. Hence $f_i = l_i \chi^{(i)}/n$.

Applying ρ to (3) and using $k_i^\rho = f_i 1$, we get

$$f_i f_j = \sum_{r=1}^{h} m_{ij}^{(r)} f_r. \tag{4}$$

Fix i and regard (4) as a system of h homogeneous linear equations in the f_j:

$$\sum_{r=1}^{h} (f_i \delta_{jr} - m_{ij}^{(r)}) f_r = 0, \qquad j = 1, 2, \ldots, h.$$

Now the f_j cannot all equal 0 because $f_1 \neq 0$ if $K_1 = \{1\}$, so the linear system has a nontrivial solution. Hence the determinant of the $h \times h$ matrix

whose (j, r) entry is $f_i\delta_{jr} - m_{ij}^{(r)}$ must vanish. This shows that f_i is a root of a monic polynomial in $\mathbb{Z}[t]$, and hence is an algebraic integer. □

8.3.11. *Let G be a finite group and let F be an algebraically closed field of characteristic* 0. *Then the degrees of the irreducible F-representations of G divide the order of the group.*

Proof. Let ρ be an irreducible F-representation of G and let χ be the character of ρ. We employ the notation of 8.3.10. Writing $|G| = m$ and K_{i*} for the conjugacy class $(K_i)^{-1}$, we have by 8.3.5

$$\frac{m}{n} = \frac{1}{n}\sum_{x\in G}(x)\chi(x^{-1})\chi = \frac{1}{n}\sum_{i=1}^{h} l_i\chi^{(i)}\chi^{(i*)}.$$

Since $f_i = l_i\chi^{(i)}/n$, this becomes $m/n = \sum_{i=1}^{h} f_i\chi^{(i*)}$. Now $\chi^{(i*)}$ is the trace of an element of G and as such is a sum of roots of unity in F. Since a root of unity is certainly an algebraic integer, we can apply 8.3.10 and 8.3.8 to conclude that m/n is an algebraic integer. Finally 8.3.9 shows that m/n is an integer. □

The Character Table

Let G be a finite group and F an algebraically closed field whose characteristic does not divide $|G|$. Let $K_1, \ldots, K_h$ be the conjugacy classes of G and $\chi_1, \ldots, \chi_h$ the irreducible F-characters. The value of χ_i on K_j will be denoted by $\chi_i^{(j)}$. The values of the characters can be conveniently displayed in the *character table of G.*

	K_1	$\cdots$	K_h
χ_1	$\chi_1^{(1)}$	$\cdots$	$\chi_1^{(h)}$
$\vdots$	$\vdots$		$\vdots$
χ_h	$\chi_h^{(1)}$	$\cdots$	$\chi_h^{(h)}$

The orthogonality properties of the characters may be translated into row and column orthogonality of the character table. Consider for example

$$\sum_{x\in G}(x)\chi_i(x^{-1})\chi_j = m\delta_{ij}$$

where $m = |G|$, (see 8.3.5). On writing $l_i = |K_i|$ and $K_{i*} = (K_i)^{-1}$, this becomes

$$\sum_{r=1}^{h} l_r\chi_i^{(r)}\chi_j^{(r*)} = m\delta_{ij}, \tag{5}$$

which is referred to as *orthogonality of rows.*

Define X and Y to be the $h \times h$ matrices whose (i, r) and (r, j) entries are $\chi_i^{(r)}$ and $l_r\chi_j^{(r*)}$ respectively. Then (5) expresses the matrix equation

$XY = m1_h$. Hence X is nonsingular. After conjugation by X this becomes $YX = m1_h$. Taking (r, s) entries of each side we arrive at the equation $\sum_{i=1}^{h} l_r \chi_i^{(r^*)} \chi_i^{(s)} = m\delta_{rs}$. Now l_r divides $m = |G|$, so $l_r \neq 0$ in F and

$$\sum_{i=1}^{h} \chi_i^{(r^*)} \chi_i^{(s)} = \frac{m}{l_r} \delta_{rs}, \tag{6}$$

which expresses *orthogonality of columns.*

Finally we specialize to the case $F = \mathbb{C}$, the field of complex numbers. Let $g \in G$ and let ρ be a $\mathbb{C}$-representation of G. Now a characteristic root f of g^ρ is a complex root of unity; thus $f^{-1} = \bar{f}$, the complex conjugate. It follows that $(x^{-1})\chi = \overline{(x)\chi}$ for any $\mathbb{C}$-character χ. Equations (5) and (6) now become

$$\sum_{r=1}^{h} l_r \chi_i^{(r)} \bar{\chi}_j^{(r)} = m\delta_{ij} \quad \text{and} \quad \sum_{i=1}^{h} \bar{\chi}_i^{(r)} \chi_i^{(s)} = \frac{m}{l_r} \delta_{rs}. \tag{7}$$

Example. Let G be the quaternion group of order 8 with generators a, b and the usual relations $a^4 = 1 = b^4$, $a^2 = b^2$, $a^b = a^{-1}$. We shall determine the character table of G over $\mathbb{C}$.

The conjugacy classes of G are $K_1 = \{1\}$, $K_2 = \{a^2\}$, $K_3 = \{a, a^{-1}\}$, $K_4 = \{b, b^{-1}\}$, $K_5 = \{c, c^{-1}\}$ where $c = ab$. Hence the class number is 5.

Let $\chi_1, \dots, \chi_5$ be the irreducible characters, χ_1 being the trivial character and n_i the degree of χ_i. We know from 8.2.3 and 8.3.11 that $\sum_{i=1}^{5} n_i^2 = 8$ and each n_i divides 8. It follows that one degree is 2 and the other four are 1, say

$$n_1 = n_2 = n_3 = n_4 = 1 \quad \text{and} \quad n_5 = 2.$$

It is easy to determine the characters of degree 1 since they arise from homomorphisms of G_{ab}, a 4-group, into the multiplicative group of $\mathbb{C}$. For example $a \mapsto +1$, $b \mapsto -1$, $c \mapsto -1$ is a representation of degree 1 with character values on K_1, K_2, K_3, K_4, K_5 equal to $1, 1, 1, -1, -1$ respectively: let this character be χ_2. Two more nontrivial characters χ_3, χ_4 with degree 1 are obtained by cyclically permuting a, b, c.

To the extent of our present knowledge the character table has the form

	K_1	K_2	K_3	K_4	K_5
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	x	y	z	t

Note that $\chi_5^{(1)} = 2$ since χ_5 has degree 2. The values x, y, z, t can be computed by means of column orthogonality. Applying the second equation of (7) with $r = 1$, $s = 2$, one obtains $1 + 1 + 1 + 1 + 2x = 0$ or $x = -2$. In a similar way we find that $y = z = t = 0$ and the table is complete.

The irreducible representation of degree 2 arises from the well-known *Pauli spin matrices*:

$$a \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad c \mapsto \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

We conclude this section with a condition for a representation to be irreducible.

8.3.12. *Let χ be an F-character of a finite group G where F is an algebraically closed field of characteristic* 0. *Then χ is irreducible if and only if $\langle \chi, \chi \rangle_G = 1$.*

Proof. Necessity of the condition has already been proved (8.3.5). Assume that $\langle \chi, \chi \rangle_G = 1$. If $\chi_1, \ldots, \chi_h$ are the irreducible characters of G, we can write $\chi = l_1\chi_1 + \cdots + l_h\chi_h$ where l_i is a nonnegative integer by 8.3.3. Hence, using $\langle \chi_i, \chi_j \rangle = \delta_{ij}$, we obtain $1 = \langle \chi, \chi \rangle_G = \sum_{i=1}^{h} l_i^2$, which implies that one of the l_i equals 1 and all the others equal 0. Thus $\chi = \chi_i$ for some i. □

Exercises 8.3

1. With the notation of the orthogonality relations (7) define A to be the $h \times h$ matrix whose (i, r) entry is $\sqrt{l_r/m}\,\chi_i^{(r)}$. Prove that A is unitary, that is, $A(\bar{A})^T = 1$.

2. Show that the degree of an irreducible $\mathbb{Q}$-representation need not divide the group order, and also that $\langle \chi, \chi \rangle$ need not be 1 if χ is a $\mathbb{Q}$-irreducible character.

3. Construct the character table of A_4 over $\mathbb{C}$.

4. Show that the character tables of D_8 and Q_8 over $\mathbb{C}$ are identical.

5. Use the Pauli spin matrices to construct an irreducible $\mathbb{Q}$-representation of Q_8 with degree 4. Hence find all irreducible $\mathbb{Q}$-representations of Q_8.

6. Show that a representation of a finite group G over a field of positive characteristic p is not in general determined by its character even if $p \nmid |G|$.

7. Prove that the dimension of the vector space of all class functions of G over F equals the class number of G (where G is finite).

8. Prove that the number of real irreducible $\mathbb{C}$-characters of a finite group equals the number of conjugacy classes K_i such that $K_i = K_{i*} (\equiv K_i^{-1})$. [*Hint*: Consider the effect on the unitary matrix of Exercise 8.3.1 of permutations $\chi_i \mapsto \bar{\chi}_i$ and $K_i \mapsto K_{i*}$.]

9. (Burnside). Let G be a finite group of odd order m and class number h. Prove that $m \equiv h \bmod 16$. [*Hint*: Show first that the only real irreducible $\mathbb{C}$-character is the trivial one and then express m as the sum of the squares of the degrees of the irreducible $\mathbb{C}$-representations.]

10. Assume that the finite group G has a faithful F-representation of degree n where n is less than the smallest prime divisor of $|G|$ and F is an algebraically closed field of characteristic 0. Prove that G is abelian.

11. Let G be a simple group of order m and let p be a prime dividing m. If the class number of G exceeds m/p^2, then the Sylow p-subgroups of G are abelian. [*Hint*: Assume that p^2 divides m and write m as the sum of the squares of the degrees of the irreducible $\mathbb{C}$-representations.]

*12. Let $\chi_1, \dots, \chi_h$ be the distinct irreducible characters of a finite group G over an algebraically closed field whose characteristic does not divide $|G|$. If χ_i has degree l_i, prove that $\sum_i l_i\chi_i$ is the character of the right regular representation.

8.4. Tensor Products and Representations

Let G be a group and F a field. We consider two F-representations ρ, σ of G arising from (right) FG-modules M, N. The tensor product

$$T = M \underset{F}{\otimes} N$$

is a finite-dimensional vector space over F with dimension mn where m and n are the dimensions of M and N. We make T into a right FG-module via the rule

$$(a \otimes b)g = (ag) \otimes (bg), \qquad (a \in M, b \in N, g \in G).$$

This is a well-defined action because $(a, b) \mapsto ag \otimes bg$ is bilinear. The module T affords a representation τ of G called the *tensor product* of ρ and σ which is written

$$\tau = \rho \otimes \sigma.$$

The degree of τ is the product of the degrees of ρ and σ. By definition of the tensor product of two linear transformations $(a \otimes b)g^\tau = ag^\rho \otimes bg^\sigma = (a \otimes b)(g^\rho \otimes g^\sigma)$. Thus

$$g^\tau = g^\rho \otimes g^\sigma, \qquad g \in G.$$

Next we ask about the relation between the character of τ and those of ρ and σ. Choose F-bases $\{a_1, \dots, a_m\}$ and $\{b_1, \dots, b_n\}$ for M and N respectively and recall that the $a_i \otimes b_j$ form a basis of T. Now

$$(a_i \otimes b_j)g^\tau = a_ig^\rho \otimes b_jg^\sigma = \sum_{k=1}^{m} (g)\rho_{ik}a_k \otimes \sum_{l=1}^{n} (g)\sigma_{jl}b_l$$

where $((g)\rho_{ik})$ and $((g)\sigma_{jl})$ are the matrices representing g^ρ and g^σ. Therefore

$$(a_i \otimes b_j)g^\tau = \sum_{k,l} ((g)\rho_{ik})((g)\sigma_{jl})(a_k \otimes b_l).$$

Hence g^τ is represented by the $mn \times mn$ matrix whose $(i, j\colon k, l)$ entry is $(g)\rho_{ik}(g)\sigma_{jl}$. The character of τ can now be found since

$$\operatorname{trace}(g^\tau) = \sum_{i,j} (g)\rho_{ii}(g)\sigma_{jj} = (\operatorname{trace}(g^\rho))(\operatorname{trace}(g^\sigma)).$$

It follows that *the character of* $\rho \otimes \sigma$ *equals the product of the characters of* ρ and σ. Here, of course, the product $\alpha\beta$ of functions $\alpha, \beta: G \to F$ is defined by $(g)\alpha\beta = ((g)\alpha)((g)\beta)$.

8.4.1. *Let G be a group and F a field. Then the sum and product of F-characters are F-characters. The set of all integral linear combinations of F-characters is a commutative ring (called the character ring).*

Proof. That the sum of two characters equals the character of the direct sum of the corresponding representations is clear. The product of two characters is the character of the tensor product of the associated representations. The remaining statement is clear. □

An element of the character ring is called a *generalized character*: usually a generalized character is not a character.

Representations of Direct Products

Let F be any field and let G be a group expressed as a direct product $G = H \times K$. Let ρ and σ be F-representations of H and K. Then a corresponding F-representation of G may be constructed from ρ and σ by using tensor products.

Suppose that ρ and σ arise from an FH-module M and an FK-module N respectively. Form the tensor product

$$T = M \underset{F}{\otimes} N$$

and make T into a right FG-module by the rule

$$(a \otimes b)(x, y) = (ax) \otimes (by),$$

where $a \in M$, $b \in N$, $x \in H$, $y \in K$. Then T affords an F-representation $\rho \# \sigma$ called the *Kronecker* (*or outer tensor*) *product* of ρ and σ. The degree of $\rho \# \sigma$ equals the product of the degrees of ρ and σ. Just as for the inner tensor product one can show that if ρ has character χ and σ has character ψ, the character φ of $\rho \# \sigma$ is given by $(x, y)\varphi = (x)\chi(y)\psi$.

8.4.2. *Let F be an algebraically closed field and let* $G = H \times K$.

(i) *If* ρ *and* σ *are irreducible F-representations of H and K, then* $\rho \# \sigma$ *is an irreducible F-representation of G.*
(ii) *Assume that G is finite and the characteristic of F does not divide the order of G. If* $\{\rho_1, \dots, \rho_h\}$ *and* $\{\sigma_1, \dots, \sigma_k\}$ *are complete sets of inequivalent irreducible F-representations of H and K, then the* $\rho_i \# \sigma_r$, $i = 1, \dots, h$, $r = 1, \dots, k$, *form a complete set of inequivalent irreducible F-representations of G.*

Proof. (i) Let M and N be right modules giving rise to ρ and σ and let $\{a_1, \ldots, a_m\}$ and $\{b_1, \ldots, b_n\}$ be F-bases of M and N. Then $T = M \otimes_F N$ has the set of all $a_i \otimes b_j$ as a basis. For fixed integers i, j, r, s define ξ in $\mathrm{End}_F(M)$ and $\eta \in \mathrm{End}_F(N)$ by the rules $a_k\xi = \delta_{ki}a_j$ and $b_l\eta = \delta_{lr}b_s$. Now 8.1.8 shows that H^ρ and K^σ generate $\mathrm{End}_F(M)$ and $\mathrm{End}_F(N)$ respectively as vector spaces; hence we can write

$$\xi = \sum_{x \in H} u_x x^\rho \qquad \text{and} \qquad \eta = \sum_{y \in K} v_y y^\sigma$$

where $u_x, v_y \in F$. Then one setting $\zeta = \xi \otimes \eta$ we have

$$\zeta = \sum_{x \in H} \sum_{y \in K} u_x v_y (x^\rho \otimes y^\sigma) = \sum_{x \in H} \sum_{y \in K} u_x v_y (x, y)^\tau$$

where $\tau = \rho \# \sigma$. However, by definition of ξ and η,

$$(a_k \otimes b_l)\zeta = a_k\xi \otimes b_l\eta = \delta_{ki}\delta_{lr}(a_j \otimes b_s).$$

Thus if we allow i, j, r, s to vary, the resulting ζ's will generate $\mathrm{End}_F(T)$. But all such ζ's belong to the subspace $V = F(G^\tau)$, so $V = \mathrm{End}_F(T)$. Clearly this implies that τ is irreducible.

(ii) By (i) the $\rho_i \# \sigma_r$ are irreducible F-representations: we must show that no two of them are equivalent. Let ρ_i have character χ_i and let σ_r have character ψ_r. Then $\rho_i \# \sigma_r$ has character φ_{ir} where $(x, y)\varphi_{ir} = (x)\chi_i(y)\psi_r$. Hence

$$\begin{aligned}\langle \varphi_{ir}, \varphi_{js} \rangle_G &= \frac{1}{|H| \cdot |K|} \sum_{\substack{x \in H \\ y \in K}} (x)\chi_i(y)\psi_r(x^{-1})\chi_j(y^{-1})\psi_s \\ &= \left(\frac{1}{|H|} \sum_{x \in H} (x)\chi_i(x^{-1})\chi_j\right)\left(\frac{1}{|K|} \sum_{y \in K} (y)\psi_r(y^{-1})\psi_s\right) \\ &= \langle \chi_i, \chi_j \rangle_H \cdot \langle \psi_r, \psi_s \rangle_K \\ &= \delta_{ij}\delta_{rs},\end{aligned}$$

by 8.3.6. Therefore $\varphi_{ir} \neq \varphi_{js}$ if $(i, r) \neq (j, s)$, and the hk representations $\rho_i \# \sigma_r$ are inequivalent. But the total number of inequivalent irreducible F-representations of G equals the class number of G, which clearly equals hk (Exercise 1.6.4). Hence the $\rho_i \# \sigma_r$ constitute a complete set of inequivalent irreducible F-representations of G. □

Induced Representations

If H is a subgroup of a group G and ρ is an F-representation of G, an F-representation of H is obtained by simply restricting ρ to H. A less trivial problem is to construct a representation of G starting with a representation of H. This leads to the important concept of an induced representation, which is due to Frobenius.

Suppose that G is a group and H is a subgroup of G with finite index r. Let there be given an F-representation ρ of H arising from a right FH-module M. We proceed to form the tensor product over FH,

$$M^G = M \underset{FH}{\otimes} FG,$$

wherein FG is to be regarded as a *left* FH-module by means of left multiplication. So far M^G is only an F-module. However FG is also a *right* FG-module via right multiplication. Consequently M^G becomes a right FG-module by means of the rule

$$(a \otimes r)s = a \otimes (rs), \qquad (a \in M \text{ and } r, s \in FG).$$

The FH-bilinearity of the map $(a, r) \mapsto a \otimes (rs)$ shows this action to be well-defined.

The right FG-module M^G is called the *induced module* of M, and the F-representation which arises from M is called the *induced representation* of ρ,

$$\rho^G.$$

If ρ has character χ, we shall write χ^G for the *induced character*, that is, the character of ρ^G.

We plan now to investigate the nature of the module M^G. Choosing a right transversal $\{t_1, \ldots, t_r\}$ to H in G, we may write each element of FG uniquely in the form $\sum_{i=1}^r u_i t_i$ with u_i in FH. Hence there is a decomposition of FG into left FH-modules $FG = (FH)t_1 \oplus \cdots \oplus (FH)t_r$. By the distributive property of tensor products there is an F-isomorphism.

$$M^G \simeq M \underset{FH}{\otimes} ((FH)t_1) \oplus \cdots \oplus M \underset{FH}{\otimes} ((FH)t_r). \tag{8}$$

By virtue of the equation $a \otimes ut_i = au \otimes t_i$ where $u \in FH$, we can rewrite (8) as

$$M^G \simeq M \otimes t_1 \oplus \cdots \oplus M \otimes t_r.$$

Hence, if $\{a_1, \ldots, a_n\}$ is a basis of M over F, the elements $a_i \otimes t_j$, $i = 1, 2, \ldots, n, j = 1, 2, \ldots, r$, form a basis for M^G over F. In particular

$$\text{degree } \rho^G = (\text{degree } \rho) \cdot |G : H|.$$

On the basis of these remarks the values of the induced character χ^G can be calculated.

8.4.3. *Let G be a finite group, H a subgroup of G, and F a field whose characteristic does not divide the order of H. If χ is an F-character of H, the value of the induced character is given by*

$$(g)\chi^G = \frac{1}{|H|} \sum_{x \in G} (xgx^{-1})\chi$$

where it is understood that χ is zero on $G \backslash H$.

Proof. Let ρ be an F-representation of H with character χ. Choose a basis $\{a_1, \dots, a_n\}$ of the FH-module M giving rise to ρ and let $\{t_1, \dots, t_r\}$ be a right transversal to H in G. We have observed that the $a_i \otimes t_j$ form a basis of M^G. If $g \in G$, then $t_j g = x t_k$ for some k and $x = t_j g t_k^{-1} \in H$. Hence

$$(a_i \otimes t_j)g = a_i \otimes (t_j g) = a_i \otimes (x t_k) = (a_i x) \otimes t_k.$$

As usual $((g)\rho_{ij})$ is the matrix representing g^ρ; then

$$(a_i \otimes t_j)g = \left(\sum_{l=1}^{n} (x)\rho_{il} a_l\right) \otimes t_k = \sum_{l=1}^{n} (t_j g t_k^{-1})\rho_{il}(a_l \otimes t_k).$$

Now for given j and g there is precisely one k such that $t_j g t_k^{-1} \in H$. Hence, with the convention that ρ_{il} is zero on $G \backslash H$, one has

$$(a_i \otimes t_j)g = \sum_{l=1}^{n} \sum_{k=1}^{r} (t_j g t_k^{-1})\rho_{il}(a_l \otimes t_k).$$

This establishes that the $nr \times nr$ matrix representing g^{ρ^G} has $(i, j\colon l, k)$ entry equal to $(t_j g t_k^{-1})\rho_{il}$. The character χ^G can now be computed.

$$(g)\chi^G = \sum_{i=1}^{n} \sum_{j=1}^{r} (t_j g t_j^{-1})\rho_{ii} = \sum_{j=1}^{r} (t_j g t_j^{-1})\chi.$$

Finally, if $z \in H$,

$$(z t_j g (z t_j)^{-1})\chi = (z(t_j g t_j^{-1})z^{-1})\chi = (t_j g t_j^{-1})\chi$$

since χ is a class function H. Hence

$$(g)\chi^G = \frac{1}{|H|} \sum_{x \in G} (x g x^{-1})\chi. \qquad \square$$

The Frobenius Reciprocity Theorem

The following theorem is used quite frequently in computations with induced characters.

8.4.4 (Frobenius). *Let G be a finite group and let F be a field whose characteristic does not divide the order of G. Assume that H is a subgroup of G and that ψ and χ are F-characters of H and G respectively. Then*

$$\langle \psi^G, \chi \rangle_G = \langle \psi, \chi_H \rangle_H$$

where χ_H denotes the restriction of χ to H.

Proof. Let $|H| = l$ and $|G| = m$. Applying 8.4.3 we have

$$\langle \psi^G, \chi \rangle_G = \frac{1}{m} \sum_{x \in G} (x)\psi^G (x^{-1})\chi = \frac{1}{lm} \sum_{x \in G} \sum_{y \in G} (y x y^{-1})\psi (x^{-1})\chi.$$

Since $(x^{-1})\chi = (yx^{-1}y^{-1})\chi$, this becomes

$$\langle\psi^G, \chi\rangle_G = \frac{1}{lm}\sum_{y\in G}\sum_{x\in G}(yxy^{-1})\psi(yx^{-1}y^{-1})\chi$$

$$= \frac{1}{lm}\sum_{y\in G}\sum_{z\in G}(z)\psi(z^{-1})\chi = \frac{1}{l}\sum_{z\in G}(z)\psi(z^{-1})\chi.$$

Now according to our convention ψ vanishes on $G\backslash H$, so the final summation on z may be restricted to H and we obtain $\langle\psi^G, \chi\rangle_G = \langle\psi, \chi_H\rangle_H$. □

Permutation Representations

In 8.1 it was remarked that a permutation representation could be regarded as a linear representation over an arbitrary field. We shall now show that permutation representations arise as representations induced from the trivial representation of a subgroup.

In the following all representations are over an arbitrary field F and $\iota(G)$ is the trivial representation of a group G.

8.4.5.

(i) *If H is a subgroup with finite index in a group G, then $(\iota(H))^G$ is a transitive permutation representation of G with degree $|G:H|$.*

(ii) *If ρ is a permutation representation of a group G on a finite set and k is the number of G-orbits, then ρ is equivalent to $\iota(H_1)^G \oplus \cdots \oplus \iota(H_k)^G$ where the H_i are point stabilizers in G. In particular, if ρ is transitive, it is equivalent to some $\iota(H)^G$.*

Proof. (i) The representation $\iota(H)$ arises from the trivial right FH-module F. Thus $\iota(H)^G$ arises from $F \otimes_{FH} FG$, which has an F-basis

$$\{1 \otimes t_i | i = 1, 2, \ldots, r\}$$

where $\{t_1, \ldots, t_r\}$ is a right transversal to H in G. Let $g \in G$ and write $t_i g = ht_j$ where $h \in H$. Then $(1 \otimes t_i)g = 1 \otimes (ht_j) = (1)h \otimes t_j = 1 \otimes t_j$. In consequence g permutes the $1 \otimes t_i$ in exactly the same way as it permutes the right cosets Ht_i: it therefore acts transitively. Hence $\iota(H)^G$ is a transitive representation with degree $r = |G:H|$.

(ii) Suppose that ρ represents G on the set $\{1, 2, \ldots, n\}$. If M is a vector space with basis $\{a_1, \ldots, a_n\}$ over F, the action $a_i g = a_{ig^\rho}$ makes M into a right FG-module affording the linear representation ρ. Evidently $\rho = \rho_1 \oplus \cdots \oplus \rho_k$ where ρ_i is transitive; thus we can assume that ρ is transitive. Define H to be the stabilizer of 1 in G and put $i = 1t_i^\rho$, using transitivity. Then $\{t_1, \ldots, t_n\}$ is a right transversal to H in G. If we define $(1 \otimes t_i)\alpha$ to be a_i, this yields $\alpha: F^G \to M$, an F-isomorphism from F^G to M. Also, if $g \in G$ and $t_i g = ht_j$ with $h \in H$, then $a_i g = a_1(t_i g) = a_j = (1 \otimes t_j)\alpha = ((1 \otimes t_i)g)\alpha$. Thus α is an FG-isomorphism and ρ is equivalent to $\iota(H)^G$. □

The Character of a Permutation Group

Let G be a finite permutation group. Then G has a natural linear representation over an arbitrary field F and hence a natural F-character $\pi: G \to F$. Note that $(g)\pi$ has a simple interpretation: for if we represent g by a permutation matrix g^*, then $(g)\pi = \text{trace}(g^*)$, which is just the number of fixed points of the permutation g.

The following result shows how the permutation character may be used to construct irreducible characters of permutation groups.

8.4.6. *Let G be a finite permutation group with character π over an algebraically closed field F of characteristic 0. Let $\chi_1(G)$ be the trivial F-character of G.*

(i) *The number of G-orbits equals $\langle \pi, \chi_1(G)\rangle_G$.*
(ii) *Let G be transitive. If H is a point stabilizer in G, the number of H-orbits equals $\langle \pi, \pi\rangle_G = \sum_{x\in G}((x)\pi)^2$.*
(iii) *Let G be transitive. Then G is 2-transitive if and only if $\pi = \chi_1(G) + \chi$ where χ is an irreducible F-character of G.*

Proof. (i) Write $\pi = \pi_1 \oplus \cdots \oplus \pi_k$ where π_i is the character of a transitive permutation representation of G and k is the number of G-orbits. Then by 8.4.5 we have $\pi_i = (\chi_1(H_i))^G$ for some point stabilizer H_i in G. Therefore by 8.4.4

$$\langle \pi, \chi_1(G)\rangle_G = \sum_{i=1}^{k} \langle \chi_1(H_i)^G, \chi_1(G)\rangle_G = \sum_{i=1}^{k} \langle \chi_1(H_i), \chi_1(H_i)\rangle_{H_i} = k$$

since $(\chi_1(G))_{H_i} = \chi_1(H_i)$. (See also Exercise 1.6.2 for an elementary proof of (i).)

(ii) Let $H_1, \ldots, H_n$ be the point stabilizers in G; here of course n is the degree of G. Now $(x^{-1})\pi = (x)\pi$, so $\langle \pi, \pi\rangle_G = (1/|G|)\sum_{x\in G}((x)\pi)^2$. Also, in the sum $\sum_{i=1}^{n}\sum_{x\in H_i}(x)\pi$ the number $(x)\pi$ is counted each time that x occurs in an H_i. Since x has exactly $(x)\pi$ fixed points, we deduce that this sum equals $\sum_{x\in G}((x)\pi)^2$. Hence

$$\langle \pi, \pi\rangle_G = \frac{1}{|G|}\sum_{i=1}^{n}\sum_{x\in H_i}(x)\pi.$$

Since G is transitive, the H_i are conjugate in G and $\sum_{x\in H_i}(x)\pi$ is independent of i. If s is the number of H_1-orbits, then $\sum_{x\in H_1}(x)\pi = s|H_1|$ by (i). Hence

$$\langle \pi, \pi\rangle_G = \frac{1}{|G|}(ns|H_1|) = s.$$

(iii) Let $\chi_1, \chi_2, \ldots, \chi_h$ be the distinct irreducible F-characters of G with $\chi_1 = \chi_1(G)$. By 8.3.3 we can write $\pi = \sum_i n_i\chi_i$ (with integral $n_i \geq 0$), and using 8.3.5 we obtain $\langle \pi, \pi\rangle_G = n_1^2 + n_2^2 + \cdots + n_h^2$. Now $n_1 = \langle \pi, \chi_1\rangle_G = 1$ by (i). Hence $s = 1 + n_2^2 + \cdots + n_h^2$. Now by 7.1.1 the group G is 2-transitive if and

only if H_1 is transitive on $X\backslash\{a\}$ where G acts on X and H_1 is the stabilizer of a, that is, if and only if $s = 2$. This occurs when exactly one n_i equals 1 and $n_j = 0$ if $j \geq 2$ and $j \neq i$. Consequently $\pi = \chi_1 + \chi_i$. □

EXAMPLE. To illustrate the use of 8.4.6 in constructing irreducible representations let us consider the $\mathbb{C}$-representations of the symmetric group S_4. There are five conjugacy classes, corresponding to the different cycle types;

$$K_1: (*)(*)(*)(*), \quad K_2: (*\ *)(*)(*), \quad K_3: (*\ *)(*\ *)$$

$$K_4: (*\ *\ *)(*), \quad K_5: (*\ *\ *\ *)$$

The natural permutation character π has, of course, degree 4 and its values on the five conjugacy classes are 4, 2, 0, 1, 0, as may be seen by counting fixed points. Since G is 2-transitive, 8.4.6(iii) implies that there is an irreducible character $\chi_2 = \pi - \chi_1$: the values of χ_2 are, therefore, 3, 1, -1, 0, -1, and χ_2 has degree 3.

Now G has a 2-transitive permutation representation of degree 3 wherein its elements permute by conjugation the elements of $K_3 = \{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$. Once again counting fixed points, we conclude that the corresponding permutation character σ has values 3, 1, 3, 0, 1. By 8.4.6 again we find an irreducible character χ_3 with values 2, 0, 2, -1, 0; this has degree 2.

There is a nontrivial irreducible character of degree 1, the *sign character* χ_4 arising from the representation $x \mapsto \text{sign } x$. The values of χ_4 are 1, -1, 1, 1, -1.

The remaining irreducible character χ_5 has values which can be determined by use of the orthogonality relations (Equation (6)). The complete character table is

	K_1	K_2	K_3	K_4	K_5
χ_1	1	1	1	1	1
χ_2	3	1	-1	0	-1
χ_3	2	0	2	-1	0
χ_4	1	-1	1	1	-1
χ_5	3	-1	-1	0	1

Observe that $\chi_5 = \chi_2\chi_4$.

The representations of S_n have been extensively investigated—for details see [b55].

Monomial Representations

An F-representation ρ of a group G is called *monomial* if $\rho = \rho_1 \oplus \cdots \oplus \rho_k$ where ρ_i is induced from a representation of degree 1 of a subgroup of G. For example, it follows from 8.4.5 that *every permutation representation is monomial.*

In order to visualize a monomial representation we examine the associated matrix representation. Suppose that ρ arises from an FG-module M and that $M = M_1 \oplus \cdots \oplus M_k$ where the FG-module M_i gives rise to ρ_i. Then $M_i = N_i^G$ where N_i is an FH_i-module of dimension 1 and the H_i are subgroups of G. Write $N_i = Fa_i$ and choose a right transversal $\{t_j^{(i)} | j = 1, 2, \ldots, r_i\}$ to H_i in G, so that the $a_i \otimes t_j^{(i)}, j = 1, 2, \ldots, r_i$, form a basis of M_i. Selecting g from G, we write $t_j^{(i)}g = ht_k^{(i)}$ for a unique integer k and element h of H. Now $a_ih = c_{ij}^{(g)}a_i$ for some $c_{ij}^{(g)}$ in F^* since $N_i = Fa_i$; thus we have

$$(a_i \otimes t_j^{(i)})g = a_i \otimes (ht_k^{(i)}) = c_{ij}^{(g)}(a_i \otimes t_k^{(i)}).$$

The matrix representing g^ρ with respect to the basis of all $a_i \otimes t_j^{(i)}$ has its $(i, j\colon i, k)$ entry equal to $c_{ij}^{(g)}$, and all other entries 0. Thus $g^{\rho *}$ has precisely one nonzero element in each row and in each column.

A matrix of this sort is called a *monomial matrix*; it is clearly a generalization of a permutation matrix.

Groups whose Representations Are Monomial

A finite group G is said to be an *$\mathscr{M}$-group* if, whenever F is an algebraically closed field of characteristic not dividing $|G|$, every F-representation is monomial. By Maschke's Theorem G is an $\mathscr{M}$-group if and only if all the irreducible representations are monomial. For example, by 8.1.6 *all finite abelian groups are $\mathscr{M}$-groups.*

The following result is helpful in connection with $\mathscr{M}$-groups.

8.4.7 (Blichfeldt). *Let G be a finite group, F an algebraically closed field and M a simple FG-module which affords a faithful representation of G. Assume that G has a normal abelian subgroup A not contained in the center of G. Then there exists a proper subgroup H of G and a simple FH-module N such that M and N^G are FG-isomorphic.*

Proof. By Clifford's Theorem (8.1.3) we may write $M = M_1 \oplus \cdots \oplus M_k$ where M_i is a direct sum of isomorphic simple FA-modules and G permutes the M_i transitively. By 8.1.6 the action of A on M_i is scalar. Should k equal 1, then $A \leq \zeta G$ because G acts faithfully on M. Since this is contrary to hypothesis, $k > 1$. Set $N = M_1$ and define $H = \{g \in G | Ng = N\}$, the stabilizer of N in G. In view of the transitivity of G on the M_i we have $|G : H| = k > 1$ and $H < G$. Recall from 8.1.3 that N is a simple FH-module.

By transitivity once again, $M_i = Ng_i$ for some g_i in G and $\{g_1, \ldots, g_k\}$ is a right transversal to H in G. Finally, if $a_i \in N$, the mapping $\sum_i a_i \otimes g_i \mapsto \sum_i a_i g_i$ is an F-isomorphism from N^G to M which one easily verifies to be an FG-homomorphism. □

The next result will furnish us with some examples of $\mathscr{M}$-groups.

8.4.8. *Let G be a finite group such that if $U \lhd V \leq G$, then either V/U is abelian or it possesses a noncentral abelian normal subgroup. Then G is an $\mathscr{M}$-group.*

Proof. Let M be a simple FG-module where F is an algebraically closed field whose characteristic does not divide $|G|$. It must be shown that M is induced from a 1-dimensional module. Let ρ be the representation afforded by M and set $K = \operatorname{Ker} \rho$. Suppose first that $K \neq 1$. Then $\bar{G} = G/K$ is an $\mathscr{M}$-group by induction on $|G|$. Since K acts trivially on M, it is clear that M is also an $F\bar{G}$-module. Hence there is a subgroup $\bar{H}$ of $\bar{G}$, a 1-dimensional $F\bar{H}$-module N, and an $F\bar{G}$-isomorphism $\theta\colon M \to N^{\bar{G}}$. Since $F\bar{G}$ is a right FG-module via right multiplication, $N^{\bar{G}} = N \otimes_{F\bar{H}} F\bar{G}$ becomes a right FG-module. One verifies at once that θ is an FG-isomorphism. Now write $\bar{H} = H/K$ and note that N is an FH-module. Finally $a \otimes Kg \mapsto a \otimes g$ is an FG-isomorphism from $N^{\bar{G}}$ to N^G, and $M \simeq^{FG} N^G$.

We may therefore assume that $K = 1$ and ρ is faithful. We can also suppose that G is not abelian, otherwise it is certainly an $\mathscr{M}$-group. Then by hypothesis there is a normal abelian subgroup of G that is not contained in the center. Applying 8.4.7 we conclude that there is a proper subgroup H and a simple FH-module L such that $M \simeq^{FG} L^G$. The conditions on G are inherited by H, so by induction $L \simeq^{FH} S^H$ where S is a 1-dimensional FT-module and $T \leq H$. Hence $M \simeq L^G \simeq (S^H)^G \simeq S^G$, all isomorphisms being of right FG-modules, since $(S \otimes_{FT} FH) \otimes_{FH} FG \simeq S \otimes_{FT} FG$. (This property is called transitivity of induction—see Exercise 8.4.2.) □

8.4.9 (Huppert). *Let G be a finite soluble group and assume that G has a normal subgroup N with abelian Sylow subgroups such that G/N is supersoluble. Then G is an $\mathscr{M}$-group.*

Proof. Certainly we may assume that G is not abelian. In view of 8.4.8 it is sufficient to prove that G has a noncentral normal abelian subgroup: for quotients of subgroups inherit the hypotheses on G. Suppose that every normal abelian subgroup is contained in the centre and let A be a normal abelian subgroup which is maximal subject to $A \leq N$. Assuming that $A < N$, we let B/A be a minimal normal subgroup of G/A contained in N/A. Since G is soluble, B/A is abelian, and B is nilpotent because $A \leq \zeta G$. But $B \leq N$, so Sylow subgroups of B are abelian, and by 5.2.4 the group B itself is abelian, which contradicts the maximality of A. It follows that $A = N$ and $N \leq \zeta G$.

Since G/N is supersoluble, there is a series $N = G_0 < G_1 < \cdots < G_n = G$ such that $G_i \lhd G$ and G_{i+1}/G_i is cyclic. Now G is not abelian, so there is a least positive integer i for which $G_i \not\leq \zeta G$. Then $G_{i-1} \leq \zeta G$, and, because G_i/G_{i-1} is cyclic, G_i is abelian. Therefore $G_i \leq \zeta G$ contrary to the choice of i. □

The following corollaries of 8.4.9 are worth noting. *All finite supersoluble groups are $\mathscr{M}$-groups,* as are *all finite nilpotent groups* in particular. Also *all finite metabelian groups are $\mathscr{M}$-groups*—to see this take N in 8.4.9 to be G'.

On the other hand, it is natural to ask what can be said of the structure of $\mathscr{M}$-groups in general. We shall prove just one result.

8.4.10 (Taketa). *Every $\mathscr{M}$-group is soluble.*

Proof. Assuming the theorem to be false, we choose an insoluble $\mathscr{M}$-group G of least order. It is easy to see that a quotient group of an $\mathscr{M}$-group is also an $\mathscr{M}$-group. Thus every proper quotient group of G is soluble, by minimality of G. Define N to be the intersection of all the nontrivial normal subgroups of G. Then G/N is surely soluble, so $N \neq 1$. Applying Exercise 8.1.4 we are able to find a faithful irreducible $\mathbb{C}$-representation ρ of G; moreover we may assume that ρ has been chosen of minimal degree, which will have to exceed 1 otherwise G would be abelian. By hypothesis ρ is monomial. Replacing each nonzero element of the monomial matrix g^{ρ^*} by 1, we obtain a permutation matrix and so a permutation representation σ of G. The degree of σ equals that of ρ and hence exceeds 1. Now by Exercise 8.1.2 the representation σ is reducible. Thus an irreducible component of σ has smaller degree than ρ and hence cannot be faithful. Since N is contained in every nontrivial normal subgroup of G, it follows that N is contained in $K = \operatorname{Ker} \sigma$. But, if $x \in K$, then x^{ρ^*} is a diagonal matrix, which implies that K^ρ is abelian. Since $K \simeq K^\rho$, it follows that K, and hence N, is abelian. Thus G is soluble, which is a contradiction. □

Example. *Not every finite soluble group is an $\mathscr{M}$-group.* Let $Q = \langle a, b, c\rangle$ be a quaternion group of order 8, the three subgroups of order 4 being $\langle a\rangle$, $\langle b\rangle$, and $\langle c\rangle$. There is an automorphism τ of Q which permutes a, b, c cyclically and has order 3. Define G to be the semidirect product of Q by $\langle\tau\rangle$. Then G has order 24 and is soluble with derived length 3: actually $G \simeq$ SL(2, 3).

The following assignments determine a $\mathbb{C}$-representation of G with degree 2,

$$a \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad c \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

$$\tau \mapsto 2^{-1}(i-1)\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}, \qquad \text{where} \quad i = \sqrt{-1},$$

as simple matrix calculations show. It is also clear that ρ is faithful; hence ρ is irreducible since otherwise G would be abelian. If ρ were monomial, it would have to be induced from a representation of a subgroup of index 2. However $G' = Q$, so $|G_{\mathrm{ab}}| = 3$ and there are no subgroups of index 2 in G. Consequently G is not an $\mathscr{M}$-group.

We conclude by mentioning a theorem of Dade which indicates that the structure of an $\mathscr{M}$-group can be very complex: *every finite soluble group is isomorphic with a subgroup of an $\mathscr{M}$-group.* Further results on $\mathscr{M}$-groups can be found in [b6].

EXERCISES 8.4

1. Let H and K be subgroups of a finite group G. Let $\chi_1(H)$ and $\chi_1(K)$ denote the trivial characters of H and K over an algebraically closed field of characteristic 0. Prove that $\langle \chi_1(H)^G, \chi_1(K)^G \rangle_G$ equals the number of (H, K)-double cosets.
2. Let $H \leq K \leq G$ where G is finite. Let M be an FH-module, where F is any field. Show that $(M^K)^G \simeq^{FG} M^G$ (*transitivity of induction*).
3. (i) Show that every generalized character is a difference of characters; (ii) give an example of a generalized character that is not a character.
4. Let $G = D_{14}$ be the dihedral group of order 14. By forming induced representations of the subgroup of order 7 construct the $\mathbb{C}$-character table of G.
5. Find three irreducible $\mathbb{C}$-characters of A_5 by using induced representations. Hence construct the character table with the aid of orthogonality relations.
6. Let H be a subgroup with index m in the finite group G. Let F be an algebraically closed field of characteristic 0. If χ is an irreducible F-character of G with degree n, show that there is an irreducible F-character φ with degree at least n/m. If H is abelian, deduce that no irreducible F-character of G has degree greater than m. [*Hint*: Let ψ be an irreducible character of H that is a direct summand of χ_H and consider $\langle \chi, \psi^G \rangle_G$.]
7. Let G be a transitive finite permutation group with permutation character π. If χ is an irreducible $\mathbb{C}$-character, prove that its degree is at least $\langle \pi, \chi \rangle_G$.
8. Let χ be an irreducible $\mathbb{C}$-character of a finite group G and let K denote the kernel of the associated representation. If χ has degree n, prove that $(x)\chi = n$ if and only if $x \in K$.
9. Let χ be a faithful $\mathbb{C}$-character of the finite group G with degree n. Denote by r the number of distinct values assumed by χ. Prove that each irreducible $\mathbb{C}$-character occurs as a direct summand of at least one power χ^s, $s = 0, 1, \ldots, r-1$ (here χ^0 is the trivial character). Deduce that the sum of the degrees of the irreducible $\mathbb{C}$-representations cannot exceed $(n^r - 1)/(n - 1)$. [*Hint*: Let ψ be an irreducible $\mathbb{C}$-character and show that not every $\langle \chi^s, \psi \rangle_G$ can be 0.]

8.5. Applications to Finite Groups

Enough representation theory has been developed to prove three celebrated and powerful theorems about finite groups due to Burnside, Frobenius, and Wielandt. Each of these is a criterion for the nonsimplicity of a group.

We approach Burnside's theorem through a lemma.

8.5.1. *Let ρ be an irreducible representation of degree n of a finite group G over the complex field $\mathbb{C}$. Denote the character of ρ by χ. Suppose that g is an element of G with exactly l conjugates and that $(l, n) = 1$. Then either $(g)\chi = 0$ or g^ρ is scalar.*

Proof. We saw in 8.3.10 that $l(g)\chi/n$ is an algebraic integer. Since $(l, n) = 1$, there are integers r and s such that $1 = rl + sn$. Hence by 8.3.8

$$t = \frac{(g)\chi}{n} = \frac{rl(g)\chi}{n} + s(g)\chi$$

is an algebraic integer.

Let $f_1, \dots, f_n$ be the characteristic roots of g^ρ, so that $(g)\chi = f_1 + \cdots + f_n$ and $|t| = |\sum_{i=1}^n f_i|/n$. Since each f_i is a root of unity, $|f_i| = 1$ and hence $|t| \le 1$. Suppose that the f_i are *not* all equal; then $|t| = |\sum_{i=1}^n f_i|/n < 1$. Let α be an automorphism of the field $\mathbb{Q}(f_1, \dots, f_n)$; then the f_i^α are not all equal, so $|t^\alpha| < 1$ in the same way. Thus the product u of all the t^α satisfies $|u| < 1$. However $u^\alpha = u$ for all automorphisms α. By the fundamental theorem of Galois theory $u \in \mathbb{Q}$. But u is an algebraic integer since t is; thus u is an integer by 8.3.9. Hence $u = 0$ and therefore $t = 0$, which shows that $(g)\chi = 0$.

Finally, if the f_i are all equal, then g^ρ is scalar, as may be seen by applying Maschke's Theorem to the restriction of ρ to $\langle g \rangle$. □

8.5.2 (Burnside). *If the finite group G has a conjugacy class with exactly $p^m > 1$ elements where p is prime, then G is not simple.*

Proof. Assume that G is simple—of course G cannot be abelian. Let g in G have p^m conjugates. Suppose that ρ is a nontrivial irreducible $\mathbb{C}$-representation of G with character χ; assume $(g)\chi \neq 0$ and that p does not divide the degree of χ. Then it follows from 8.5.1 that g^ρ is scalar and hence central in G^ρ. But G is simple and ρ is not the trivial representation, so Ker $\rho = 1$ and $G \simeq G^\rho$. Consequently $g = 1$, which gives the contradiction $p^m = 1$. Hence $(g)\chi = 0$ for every nontrivial irreducible character χ whose degree is prime to p.

Let ψ be the character of the right regular representation σ of G. Then by Exercise 8.3.12 we can write $\psi = \sum_i l_i \chi_i$ where $\chi_1, \dots, \chi_h$ are the distinct irreducible $\mathbb{C}$-characters of G and l_i is the degree of χ_i. Thus $l_1 = 1$ if χ_1 is the trivial character. It follows from the previous paragraph that $(g)\psi \equiv 1 \bmod p$. However g^σ has no fixed points, which implies that $(g)\psi = 0$: we have reached a contradiction. □

The famous solubility criterion of Burnside is now easily attained.

8.5.3 (The Burnside p-q Theorem). *If p and q are primes, a group of order $p^m q^n$ is soluble.*

Proof. Suppose the theorem to be false and choose a counterexample G of smallest order. If N were a proper nontrivial normal subgroup, both N and G/N would be soluble by minimality of G; thus G would be soluble. Consequently G must be simple. Let Q be a Sylow q-subgroup of G; then $Q \neq 1$ since certainly G cannot be a p-group. Choose a nontrivial element g in ζQ (using 1.6.14). Then $|G : C_G(g)|$ equals a power of p greater than 1 since $Q \leq C_G(g) \neq G$. However, this is impossible by 8.5.2. □

Remark. Wielandt and Kegel have proved that a finite group which is the product of two nilpotent subgroups is soluble. This represents a generalization of 8.5.3. For a proof see [b6].

The Frobenius–Wielandt Theorems

8.5.4 (Wielandt). *Suppose that G is a finite group with subgroups H and K such that $K \lhd H$ and $H \cap H^x \leq K$ for all x in $G \backslash H$. Let N be the set of elements of G which do not belong to any conjugate of $H \backslash K$. Then N is a normal subgroup of G such that $G = HN$ and $H \cap N = K$.*

This is perhaps the most famous of all criteria for nonsimplicity, especially the case $K = 1$, which is due to Frobenius.

Proof. (i) Observe that if $H = K$, then $N = G$ and the result is certainly true. We assume henceforth that $K < H$. Write $|H| = h$, $|K| = k$, and $|G| = m$.

(ii) It is sufficient to prove that N is a subgroup; for suppose that this has been accomplished. Then $N \lhd G$ since clearly $g^{-1}Ng = N$ for all g in G. If $x \in N_G(H)$, one has $K < H = H \cap H^x$, whence $x \in H$ by the hypothesis and H is self-normalizing. It follows that if $\{t_1, \ldots, t_r\}$ is a right transversal to H in G, then $H^{t_1}, \ldots, H^{t_r}$ are the distinct conjugates of H. Since $H \cap H^{t_i t_j^{-1}} \leq K$ if $i \neq j$, the subsets $(H\backslash K)^{t_i}$ are mutually disjoint. Now any g in G may be written in the form ht_i with $h \in H$; thus $(H\backslash K)^g = (H\backslash K)^{t_i}$ since $K \lhd H$. Therefore $U = \bigcup_{g \in G}(H\backslash K)^g$ equals $\bigcup_{i=1}^{r}(H\backslash K)^{t_i}$, which has exactly $r(h-k)$ elements. Since $m = rh$, we obtain $|N| = |G| - |U| = rk$. Now $K \cap (H\backslash K)^g = \varnothing$; this is clear if $g \in H$, while if $g \notin H$, we have $K \cap (H\backslash K)^g \subseteq ((H^{g^{-1}} \cap H)\backslash K)^g$, which is empty because $H^{g^{-1}} \cap H \leq K$. Consequently $K \leq H \cap N$; but $H \cap N \leq K$ is clear, so $H \cap N = K$. Therefore $|HN| = |H| \cdot |N|/|H \cap N| = m = |G|$ and $G = HN$.

(iii) *Introduction of character theory* (all characters are over $\mathbb{C}$). Consider an irreducible nontrivial representation of H which maps K to 1—such certainly exist since $K \lhd H$. Let ψ be the character of the representation. Then $f = (1)\psi$ is the degree of ψ and also $(x)\psi = f$ for all x in K. We introduce a function $\varphi: H \to \mathbb{C}$ defined by

$$\varphi = f\psi_1 - \psi$$

where ψ_1 is the trivial character of H. Then φ is a class function on H and $(x)\varphi = 0$ for all x in K. Define $\varphi^*: G \to \mathbb{C}$ by

$$\varphi^* = f\psi_1^G - \psi^G; \tag{9}$$

this is a class function on G.

(iv) *The restriction of φ^* to H equals φ.* By 8.4.3 and the definition of φ^* we have

$$(y)\varphi^* = \frac{1}{h} \sum_{x \in G} (xyx^{-1})\varphi \tag{10}$$

where it is understood that ψ_1 and ψ are 0 outside H. Let $y \in H$. If $(xyx^{-1})\varphi \neq 0$, then xyx^{-1} must belong to $H \backslash K$ since φ is 0 on $G \backslash H$ and K. In this event $xyx^{-1} \in (H \cap H^{x^{-1}}) \backslash K$, so that $x \in H$. Hence $(y)\varphi^* = (1/h)\sum_{x \in H}(xyx^{-1})\varphi = (y)\varphi$ since φ is a class function on H.

(v) $\langle \varphi^*, \varphi^* \rangle_G = \langle \varphi, \varphi \rangle_H = f^2 + 1$. Since φ is zero on N, so is φ^* by (10). Therefore

$$\langle \varphi^*, \varphi^* \rangle_G = \frac{1}{m} \sum_{x \in G} (x)\varphi^* (x^{-1})\varphi^* = \frac{1}{m} \sum_{x \in G \backslash N} (x)\varphi^* (x^{-1})\varphi^*. \tag{11}$$

Now φ^* is a class function on G, so $(x^{t_i})\varphi^* = (x)\varphi^* = (x)\varphi$ if $x \in H$. Since $G \backslash N$ is the union of all the $(H \backslash K)^{t_i}$, equation (11) becomes

$$\langle \varphi^*, \varphi^* \rangle_G = \frac{|G:H|}{|G|} \sum_{x \in H} (x)\varphi \cdot (x^{-1})\varphi = \langle \varphi, \varphi \rangle_H$$

—keep in mind that $|G:H|$ is the number of conjugates of H in G. Finally $\langle \varphi, \varphi \rangle_H = f^2 + 1$ by definition of φ.

(vi) *ψ is the restriction to H of some irreducible character ψ' of G.* Let $\chi_1, \ldots, \chi_s$ be the distinct irreducible characters of G, the trivial character being χ_1. Since φ^* is a class function, we can write $\varphi^* = \sum_{i=1}^{s} c_i \chi_i$ where $c_i = \langle \varphi^*, \chi_i \rangle_G = f\langle \psi_1^G, \chi_i \rangle_G - \langle \psi^G, \chi_i \rangle_G$, which is an integer (by 8.3.3). Moreover by the Frobenius Reciprocity Theorem (8.4.4)

$$\begin{aligned} c_1 &= f\langle \psi_1^G, \chi_1 \rangle_G - \langle \psi^G, \chi_1 \rangle_G \\ &= f\langle \psi_1, \psi_1 \rangle_H - \langle \psi, \psi_1 \rangle_H \\ &= f \end{aligned}$$

since $\psi \neq \psi_1$. Also,

$$\sum_{i=1}^{s} c_i^2 = \langle \varphi^*, \varphi^* \rangle_G = f^2 + 1$$

by (v). Therefore $\sum_{i=2}^{s} c_i^2 = 1$ and some $c_i = \pm 1$, all other c_j's being 0 if $j > 1$. Thus $\varphi^* = f\chi_1 \pm \chi_i$. Now $(1)\varphi^* = (1)\varphi = 0$ by (iv), whence $0 = f \pm (1)\chi_i$. This shows that the negative sign is the correct one and $(1)\chi_i = f$. Therefore $\varphi^* = f\chi_1 - \chi_i$. If $x \in H$, we have $(x)\chi_i = f - (x)\varphi^* = f - (x)\varphi = (x)\psi$. Hence $(\chi_i)_H = \psi$ and we can take ψ' to be χ_i.

(vii) Let Ψ denote the set of all nontrivial irreducible characters of H that are constant on K. Define $I = \bigcap \operatorname{Ker} \psi'$, the intersection being formed

over all ψ in Ψ: here, of course, Ker ψ' means the kernel of the associated representation. Clearly $I \lhd G$. We shall show that $I = N$, thus completing the proof.

Let $x \in N$ and $\psi \in \Psi$. Then $0 = (x)\varphi^*$ where φ^* is given by (9). Hence $(x)\psi' = f$ since $\varphi^* = f\chi_1 - \psi'$. Let ρ be the representation of G with character ψ'; then the characteristic roots of x^ρ, which are roots of unity, add up to f, the degree of ρ. Therefore these characteristic roots all equal 1. Applying Maschke's Theorem and 8.1.6 to $\rho|_{\langle x\rangle}$, we conclude that $x^\rho = 1$ and thus $x \in \text{Ker}\,\rho$. Hence $x \in I$ and $N \subseteq I$.

Finally let $x \in H\backslash K$. Then there is a nontrivial irreducible representation σ of H, constant on K, that does not map x to 1—otherwise by Maschke's Theorem xK would belong to the kernel of the regular representation, which, of course, is faithful. If the character of σ is ψ, then $x \notin \text{Ker}\,\psi$, whence $x \notin \text{Ker}\,\psi'$ and $x \notin I$. Thus I contains no element of $(H/K)^g$ for any g, from which it follows that $I \subseteq N$ and $I = N$. □

Frobenius Groups

The most important case of 8.5.4 is when $K = 1$.

8.5.5 (Frobenius). *If G is a finite group with a subgroup H such that $H \cap H^x = 1$ for all x in $G\backslash H$, then $N = G\backslash\bigcup_{x\in G}(H\backslash 1)^x$ is a normal subgroup of G such that $G = HN$ and $H \cap N = 1$.*

A group G which has a proper nontrivial subgroup H with the above property is called a *Frobenius group*. H is called a *Frobenius complement* and N the *Frobenius kernel*. We shall prove in Chapter 10 the important theorem of Thompson that N is always nilpotent.

Frobenius groups arise in a natural way as transitive permutation groups—for example, we observed in 7.1 that the group $H(q)$ is a Frobenius group. In fact there is a characterization of Frobenius groups in terms of permutation groups.

8.5.6.

(i) *If G is a Frobenius group with complement H, the action of G on the right cosets of H yields a faithful representation of G as a transitive nonregular permutation group in which no nontrivial element has more than one fixed point.*

(ii) *Let G be a transitive but nonregular permutation group in which no nontrivial element has more than one fixed point. Then G is a Frobenius group. The Frobenius kernel consists of 1 and all elements of G with no fixed points.*

Proof. (i) Suppose that g in G fixes two distinct right cosets Hx and Hy. Then $Hxg = Hx$ and $Hyg = Hy$, equations which imply that $g \in H^x \cap H^y$. Since $yx^{-1} \notin H$, this yields $g = 1$.

(ii) Let G act on a set X. Choose a from X and write $H = \mathrm{St}_G(a)$. If $g \in G\backslash H$, then $H \cap H^g$ consists of the elements of G that fix the distinct points a and ag. Hence $H \cap H^g = 1$ and G is a Frobenius group. The statement about the Frobenius kernel follows from the definition. □

Exercises 8.5

1. Prove the following generalization of the Burnside p-q Theorem: a finite group with a nilpotent subgroup of prime-power index is soluble.
2. The center of a Frobenius group is always trivial.
3. The dihedral group D_{2n} is a Frobenius group if and only if n is odd and > 1.
4. Let P be an extra-special group of exponent 7 and order 7^3. Let a and b be generators and put $c = [a, b]$. The assignments $a \mapsto a^2c$, $b \mapsto b^2$, $c \mapsto c^4$ determine an automorphism of order 3. Show that the semidirect product $\langle \alpha \rangle \ltimes P$ is a Frobenius group with nonabelian kernel.
5. Let G be a Frobenius group with kernel N. Prove that $C_G(x) \leq N$ for all $1 \neq x \in N$.
6. If G is a Frobenius group with kernel N, then $|G : N|$ divides $|N| - 1$.
7. Let G be a Frobenius group with kernel N. If $L \lhd G$, prove that either $L \leq N$ or $N \leq L$. [*Hint*: Assume that $L \nleq N$ and show that $|N|$ divides $|L|$.]

CHAPTER 9

Finite Soluble Groups

The foundations of the theory of finite soluble groups were laid in an influential series of papers by P. Hall between 1928 and 1937. After 1950 the subject developed further thanks to the work of R.W. Carter, W. Gaschütz, B. Huppert, and others. This activity has resulted in a theory of great elegance. Here we can only present a small part of this theory; for a complete account see the recently published book [b19].

9.1. Hall π-Subgroups

Let G be a group and let π be a nonempty set of primes. A *Sylow π-subgroup* of G is defined to be a maximal π-subgroup. While Sylow π-subgroups always exist, they are usually not conjugate if π contains more than one prime.

A more useful concept is that of a Hall π-subgroup. If G is a finite group, a π-subgroup H such that $|G:H|$ is a π'-number is called a *Hall π-subgroup* of G. It is rather obvious that every Hall π-subgroup is a Sylow π-subgroup. In general, however, G need not contain any Hall π-subgroups. For example, a Hall $\{3, 5\}$-subgroup of A_5 would have index 4, but A_5 has no such subgroups (why?). We shall shortly see that in a finite soluble group Hall π-subgroups always exist and form a single conjugacy class. Notice that the terms "Hall p-subgroup" and "Sylow p-subgroup" are synonymous for finite groups in view of Sylow's Theorem.

The *normal* π-subgroups of a group G play a special role. Suppose that H and K are π-subgroups and $K \lhd G$. Then clearly $H \cap K$ and HK/K are π-groups, from which it follows that HK is a π-group. Consequently the

subgroup generated by all the normal π-subgroups of G is a π-group. This is the unique maximum normal π-subgroup of G; it is denoted by

$$O_\pi(G).$$

The following properties of this subgroup are useful.

9.1.1. *Let G be any group and π a set of primes.*

(i) *If H is a subnormal π-subgroup of G, then $H \leq O_\pi(G)$.*
(ii) *$O_\pi(G)$ is the intersection of all the Sylow π-subgroups of G.*

Proof. (i) By hypothesis there is a series $H = H_0 \lhd H_1 \lhd \cdots \lhd H_l = G$. If $l \leq 1$, then $H \lhd G$ and $H \leq O_\pi(G)$ by definition. Assuming that $l > 1$, we have by induction on l that $H \leq O_\pi(H_{l-1})$. But the latter subgroup is characteristic in H_{l-1} and hence normal in G. Thus $O_\pi(H_{l-1}) \leq O_\pi(G)$ and $H \leq O_\pi(G)$.

(ii) Let $R = O_\pi(G)$ and let S be a Sylow π-subgroup of G. Then RS is a π-group, by the argument of the paragraph preceding this proof; therefore $R \leq S$ by maximality of S. On the other hand, the intersection of all the Sylow π-subgroups is certainly normal in G, so it is contained in R. □

In particular it follows that $O_\pi(G)$ is contained in every Hall π-subgroup of G.

The Schur–Zassenhaus Theorem

The following theorem must be reckoned as one of the truly fundamental results of group theory.

9.1.2 (Schur, Zassenhaus). *Let N be a normal subgroup of a finite group G. Assume that $|N| = n$ and $|G : N| = m$ are relatively prime. Then G contains subgroups of order m and any two of them are conjugate in G.*

We pause to introduce a useful piece of terminology. If H is a subgroup of a group G, a subgroup K is called a *complement* of H in G if

$$G = HK \qquad \text{and} \qquad H \cap K = 1.$$

The reader will recognize that 9.1.2 simply asserts that complements of N exist and any two are conjugate. There is yet another formulation of 9.1.2: if π is the set of prime divisors of m, then Hall π-subgroups of G exist and any two are conjugate.

***Proof of* 9.1.2.** (i) *Case*: *N abelian.* Let $Q = G/N$. Since N is abelian, it can be made into a Q-module via the well-defined action $a^{Ng} = a^g$. From each coset x in Q we choose a representative t_x, so that the set $\{t_x | x \in Q\}$ is a

transversal to N in G. Since $t_x t_y$ belongs to the coset $t_x t_y N = t_{xy}N$, there is an element $c(x, y)$ of N such that

$$t_x t_y = t_{xy}c(x, y).$$

By applying this equation and the associative law $(t_x t_y)t_z = t_x(t_y t_z)$ one obtains the relation

$$c(xy, z)\cdot c(x, y)^z = c(x, yz)\cdot c(y, z), \tag{1}$$

which holds for all x, y, and z in Q.

Next consider the element of N

$$d(y) = \prod_{x\in Q} c(x, y).$$

Forming the product of the equations (1) over all x in Q, we find that $d(z)\cdot d(y)^z = d(yz)\cdot c(y, z)^m$ because N is abelian; thus

$$d(yz) = d(y)^z d(z)c(y, z)^{-m}. \tag{2}$$

Since $(m, n) = 1$, there is an element $e(y)$ of N such that $e(y)^m = d(y)^{-1}$, and (2) becomes $e(yz)^{-m} = (e(y)^z e(z)c(y, z))^{-m}$. Hence

$$e(yz) = e(y)^z e(z)c(y, z).$$

We define s_x to be $t_x e(x)$ and compute

$$s_y s_z = t_y t_z e(y)^z e(z) = t_{yz}c(y, z)e(y)^z e(z) = t_{yz}e(yz) = s_{yz}.$$

Consequently the mapping $x \mapsto s_x$ is a homomorphism $\theta\colon Q \to G$. Now $s_x = 1$ implies that $t_x \in N$ and $x = N = 1_Q$. Hence θ is injective, $\operatorname{Im}\theta \simeq Q$, and $|\operatorname{Im}\theta| = m$.

Now suppose that H and H^* are two subgroups of order m. Then $G = HN = H^*N$ and $H \cap N = 1 = H^* \cap N$. Let x in Q map to u_x and u_x^* respectively under the canonical homomorphisms $Q = HN/N \to H$ and $Q = H^*N/N \to H^*$. Then $u_x^* = u_x a(x)$ where $a(x) \in N$. But $u_{xy}^* = u_x^* u_y^* = u_x a(x) u_y a(y) = u_{xy}a(x)^y a(y)$, whence we deduce the relation

$$a(xy) = a(x)^y a(y). \tag{3}$$

Define $b = \prod_{x\in Q} a(x)$. Forming the product of the equations (3) over all x in Q, we obtain $b = b^y a(y)^m$. Since $(m, n) = 1$, it is possible to write $b = c^m$ with c in N. Then the preceding equation becomes $c = c^y a(y)$ or $a(y) = c^{-y}c$. Therefore $u_y^* = u_y a(y) = u_y c^{-y} c = c^{-1}u_y c$, because $c^{-y} = (c^{-1})^{u_y}$. Hence $H^* = c^{-1}Hc$.

(ii) *Existence—The general case.* We use induction on $|G|$. Let p be a prime dividing $|N|$ and P a Sylow p-subgroup of N. Write $L = N_G(P)$ and $C = \zeta P$. Then $L \leq N_G(C) = M$, say, since C is characteristic in P. By the Frattini argument (5.2.14) we have $G = LN$ and *a fortiori* $G = MN$. Let N_1 denote the normal subgroup $N \cap M$ of M and observe that $|M : N_1| = |G : N| = m$. We may apply the induction hypothesis to the group M/C on

noting that $C \neq 1$. Let X/C be a subgroup of M/C with order m. Since $|X:C| = m$ is relatively prime to $|C|$, we can apply (i) to conclude that X has a subgroup of order m.

(iii) *Conjugacy—The case G/N soluble.* Denote by π the set of prime divisors of m and write $R = O_\pi(G)$. Let H and K be two subgroups of G both of which have order m. Then $R \leq H \cap K$ since H and K are Hall π-subgroups of G. Evidently we may pass to the group G/R. Observe that $O_\pi(G/R) = 1$, so we may as well suppose that $R = 1$. Of course we can also assume that $m > 1$, so that $N \neq G$.

Let L/N be a minimal normal subgroup of G/N. Since the latter is soluble, L/N is an elementary abelian p-group for some prime p in π. Now $H \cap L$ is a Sylow p-subgroup of L because $H \cap L \simeq (H \cap L)N/N \leq L/N$ and $|L:H \cap L| = |HL:H|$ is a p'-number. The same is true of $K \cap L$. Thus Sylow's Theorem may be applied to give $H \cap L = (K \cap L)^g = K^g \cap L$ for some g in G. Writing S for $H \cap L$, we conclude that $S \lhd \langle H, K^g \rangle = J$, say.

Suppose that $J = G$, so that $S \lhd G$. Then, because S is a π-group, $S \leq R = 1$; thus L is a p'-group. However this cannot be true since L/N is a p-group. It follows that $J \neq G$. We can now use induction on $|G|$ to conclude that H and K^g are conjugate in J, whence we derive the conjugacy of H and K.

(iv) *Conjugacy—The case N soluble.* If H and K are subgroups of G with order m, then HN'/N' and KN'/N' are conjugate by (i). Hence $H^g \leq KN'$ for some g in G. By induction on the derived length of N we conclude that H^g and K are conjugate, being subgroups of order m in the group KN'. Hence H and K are conjugate.

(v) *Conjugacy—The general case.* Since the integers m and n are relatively prime, at least one of them is odd, and the Feit–Thompson Theorem (see the discussion following 5.4.1) implies that either N or G/N is soluble. The result now follows from (iii) and (iv). □

Notice that the Feit–Thompson Theorem is only required to prove conjugacy, and then only if we do not know *a priori* that either N or G/N is soluble.

The following corollary of 9.1.2 is important.

9.1.3. *With the notation of* 9.1.2, *let m_1 be a divisor of m. Then a subgroup of G with order m_1 is contained in a subgroup of order m.*

Proof. Let H and H_1 be subgroup of G with orders m and m_1 respectively. Then $G = HN$ and $H_1N = (H_1N) \cap (HN) = ((H_1N) \cap H)N$, which shows that the order of $(H_1N) \cap H$ equals $|H_1N:N| = |H_1| = m_1$. By 9.1.2 we conclude that $H_1 = ((H_1N) \cap H)^g \leq H^g$ for some g in G; of course $|H^g| = m$. □

π-Separable Groups

Let G be a finite group and let π be a nonempty set of primes. Then G is said to be *π-separable* if it has a series each factor of which is either a π-group or a π'-group. For example, *a finite soluble group is π-separable for all π*: to see this one simply refines the derived series by inserting the π-component of each factor. Notice that π-separability is identical with π'-separability. It is also very easy to prove that every subgroup and every image of a π-separable group are likewise π-separable.

The Upper $\pi'\pi$-Series

If G is an arbitrary group, the *upper $\pi'\pi$-series* is generated by repeatedly applying $O_{\pi'}$ and O_{π}. This is, then, the series

$$1 = P_0 \lhd N_0 \lhd P_1 \lhd N_1 \lhd \cdots \lhd P_m \lhd N_m \cdots$$

defined by

$$N_i/P_i = O_{\pi'}(G/P_i) \qquad \text{and} \qquad P_{i+1}/N_i = O_{\pi}(G/N_i).$$

It is somtimes convenient to write the first few terms $N_0, P_1, N_1, \ldots$ as

$$O_{\pi'}(G), \quad O_{\pi'\pi}(G), \quad O_{\pi'\pi\pi'}(G), \ldots .$$

What we have here is a series of characteristic subgroups whose factors are alternately π'-groups and π-groups.

9.1.4. *Let G be a finite π-separable group and let $1 = H_0 \lhd K_0 \lhd H_1 \lhd K_1 \lhd \cdots \lhd H_m \lhd K_m = G$ be a $\pi'\pi$-series, that is, such that K_i/H_i is a π'-group and H_{i+1}/K_i is π-group. Then $H_i \leq P_i$ and $K_i \leq N_i$ where P_i and N_i are terms of the upper $\pi'\pi$-series of G. In particular, $N_m = G$.*

Proof. Suppose that the inclusion $H_i \leq P_i$ has been proved—it is of course true if $i = 0$. Then K_iP_i/P_i is a subnormal π'-subgroup of G/P_i, whence $K_i \leq N_i$ by 9.1.1(i). Thus $H_{i+1}N_i/N_i$ is a subnormal π-subgroup of G/N_i and $H_{i+1} \leq P_{i+1}$. The result now follows by induction. □

It follows that *a finite group G is π-separable if and only if it coincides with a term of its upper $\pi'\pi$-series*. Moreover the upper $\pi'\pi$-series is a shortest $\pi'\pi$-series; its length is termed the *π-length* of G

$$l_\pi(G).$$

We take note of a simple characterization of π-separable groups.

9.1.5. *The following properties of the finite group G are equivalent:*

(i) *G is π-separable;*
(ii) *every principal factor of G is a π or a π'-group;*
(iii) *every composition factor of G is a π-group or a π'-group.*

Proof. (i) $\rightarrow$ (ii). If G is π-separable, then so is every principal factor; but the latter are characteristically simple, so by 9.1.4 each one is either a π-group or a π'-group.

(ii) $\rightarrow$ (iii). Simply refine a principal series to a composition series.

(iii) $\rightarrow$ (i). This is obvious. □

Hall π-Subgroups of π-Separable Groups

The most important property of π-separable groups is that Hall π-subgroups exist and are conjugate.

9.1.6 (P. Hall, Čunihin). *Let the finite group G be π-separable. Then every π-subgroup is contained in a Hall π-subgroup of G and any two Hall π-subgroups are conjugate in G.*

Proof. Since each π-subgroup is contained in a Sylow π-subgroup, it suffices to prove that a Sylow π-subgroup P is a Hall π-subgroup and that all such subgroups are conjugate. This will be accomplished by induction on $|G|$, which we suppose greater than 1. Let $R = O_\pi(G)$ and assume first that $R \neq 1$. Then $R \leq P$ and by induction P/R is a Hall π-subgroup of G/R. Of course it follows that P is a Hall π-subgroup of G. If Q is another Hall π-subgroup of G, then P/R and Q/R are conjugate, whence P and Q are conjugate.

Now assume that $R = 1$. Since G is π-separable and $G \neq 1$, we have $S = O_{\pi'}(G) \neq 1$. Of course PS/S is a π-group and by induction it is contained in a Hall π-subgroup Q/S of G/S. By 9.1.3 the π-subgroup P is contained in a Hall π-subgroup P^* of Q. But P is a Sylow π-subgroup, so $P = P^*$ and P is a Hall π-subgroup of Q and hence of G. If P_1 is any other Hall π-subgroup of G, then PS/S and P_1S/S are conjugate; for these are surely Hall π-subgroups of G/S. Thus $P_1^g \leq PS$ for some g in G. But now the Schur–Zassenhaus Theorem may be applied to PS to show that P and P_1^g are conjugate. □

The most important case of 9.1.6 is when G is soluble: this is the original theorem of P. Hall and we shall restate it as

9.1.7 (P. Hall). *If G is a finite soluble group, then every π-subgroup is contained in a Hall π-subgroup of G. Moreover all Hall π-subgroups of are conjugate.*

It is a remarkable fact that the converse of 9.1.7 holds: the existence of Hall π-subgroups for all π implies solubility.

9.1.8 (P. Hall). *Let G be a finite group and suppose that for every prime p there exists a Hall p'-subgroup. Then G is soluble.*

Proof. Assume that the theorem is false and let a counterexample G of smallest order be chosen. Suppose that N is a proper nontrivial normal subgroup of G. If H is a Hall p'-subgroup of G, it is evident that $H \cap N$ and HN/N are Hall p'-subgroups of N and G/N respectively. Therefore N and G/N are soluble groups by minimality of G. But this leads to the contradiction that G is soluble. Consequently G must be a simple group.

Write $|G| = p_1^{e_1} \cdots p_k^{e_k}$ where $e_i > 0$ and $p_1, \dots, p_k$ are distinct primes. Burnside's theorem (8.5.3) shows that $k > 2$. Let G_i be a Hall p_i'-subgroup of G and put $H = G_3 \cap \cdots \cap G_k$. Then $|G : G_i| = p_i^{e_i}$. By 1.3.11 we have $|G : H| = \prod_{i=3}^{k} p_i^{e_i}$, whence $|H| = p_1^{e_1} p_2^{e_2}$ and H is soluble, by Burnside's theorem once again. Let M be a minimal normal subgroup of H; then M is an elementary abelian p-group where $p = p_1$ or p_2, let us say the former. Now $|G : H \cap G_2| = p_2^{e_2} \cdots p_k^{e_k}$, so $|H \cap G_2| = p_1^{e_1}$. Thus $H \cap G_2$ is a Sylow p_1-subgroup of H and consequently $M \leq H \cap G_2 \leq G_2$. Also $|H \cap G_1| = p_2^{e_2}$ by the same reasoning. Hence $G = (H \cap G_1)G_2$ by consideration of order. It follows that $M^G = M^{G_2} \leq G_2 < G$, and M^G is a proper nontrivial normal subgroup of G. This is a contradiction. □

Minimal Nonnilpotent Groups

Our next objective is a theorem of Wielandt asserting that if a finite group has a *nilpotent* Hall π-subgroup, then all Hall π-subgroups are conjugate. In order to prove this we need to have information about minimal nonnilpotent groups. Indeed knowledge of the structure of such groups is useful in many contexts.

9.1.9 (O.J. Schmidt). *Assume that every maximal subgroup of a finite group G is nilpotent but G itself is not nilpotent. Then:*

(i) *G is soluble;*
(ii) *$|G| = p^m q^n$ where p and q are unequal primes;*
(iii) *there is a unique Sylow p-subgroup P and a Sylow q-subgroup Q is cyclic. Hence $G = QP$ and $P \lhd G$.*

Proof. (i) Let G be a counterexample of least order. If N is a proper nontrivial normal subgroup, both N and G/N are soluble, whence G is soluble. It follows that G is a simple group.

Suppose that every pair of distinct maximal subgroups of G intersects in 1. Let M be any maximal subgroup: then certainly $M = N_G(M)$. If $|G| = n$ and $|M| = m$, then M has n/m conjugates every pair of which intersect trivially. Hence the conjugates of M account for exactly $(m-1)n/m = n - n/m$ nontrivial elements. Since $m \geq 2$, we have $n - n/m \geq n/2 > (n-1)/2$: in addition it is clear that $n - n/m \leq n - 2 < n - 1$. Since each nonidentity element of G belongs to exactly one maximal subgroup, $n - 1$ is the sum of integers lying strictly between $(n-1)/2$ and $n - 1$. This is plainly impossible.

It follows that there exist distinct maximal subgroups M_1 and M_2 whose intersection I is nontrivial. Let M_1 and M_2 be chosen so that I has maximum order. Write $N = N_G(I)$. Since M is nilpotent, $I \neq N_{M_1}(I)$ by 5.2.4, so that $I < N \cap M_1$. Now I cannot be normal in G; thus N is proper and is contained in a maximal subgroup M. Then $I < N \cap M_1 \leq M \cap M_1$, which contradicts the maximality of $|I|$.

(ii) Let $|G| = p_1^{e_1} \cdots p_k^{e_k}$ where $e_i > 0$ and the p_i are distinct primes. Assume that $k \geq 3$. If M is a maximal *normal* subgroup, its index is prime since G is soluble; let us say $|G : M| = p_1$. Let P_i be a Sylow p_i-subgroup of G. If $i > 1$, then $P_i \leq M$ and, since M is nilpotent, it follows that $P_i \lhd G$; also the subgroup $P_1 P_i$ cannot equal G since $k \geq 3$. Hence $P_1 P_i$ is nilpotent and thus $[P_1, P_i] = 1$ (by 5.2.4). It follows that $N_G(P_1) = G$ and $P_1 \lhd G$. This means that all Sylow subgroups of G are normal, so G is nilpotent. By this contradiction $k = 2$ and $|G| = p_1^{e_1} p_2^{e_2}$. We shall write $p = p_2$ and $q = p_1$.

(iii) Let there be a maximal normal subgroup M with index q. Then the Sylow p-subroup P of M is normal in G and is evidently also a Sylow p-subgroup of G. Let Q be a Sylow q-subgroup of G. Then $G = QP$. Suppose that Q is not cyclic. If $g \in Q$, then $\langle g, P \rangle \neq G$ since otherwise $Q \simeq G/P$, which is cyclic. Hence $\langle g, P \rangle$ is nilpotent and $[g, P] = 1$. But this means that $[P, Q] = 1$ and $G = P \times Q$, a nilpotent group. Hence Q is cyclic. □

Wielandt's Theorem on Nilpotent Hall π-Subgroups

In an insoluble group Hall π-subgroups, even if they exist, may not be conjugate: for example, the simple group PSL(2, 11) of order 660 has subgroups isomorphic with D_{12} and A_4: these are nonisomorphic Hall $\{2, 3\}$-subgroups and they are certainly not conjugate. However the situation is quite different when a nilpotent Hall π-subgroup is present.

9.1.10 (Wielandt). *Let the finite group G possess a nilpotent Hall π-subgroup H. Then every π-subgroup of G is contained in a conjugate of H. In particular all Hall π-subgroups of G are conjugate.*

Proof. Let K be a π-subgroup of G. We shall argue by induction on $|K|$, which can be assumed greater than 1. By the induction hypothesis a maxi-

mal subgroup of K is contained in a conjugate of H and is therefore nilpotent. If K itself is not nilpotent, 9.1.9 may be applied to produce a prime q in π dividing $|K|$ and a Sylow q-subgroup Q which has a normal complement L in K. Of course, if K is nilpotent, this is still true by 5.2.4.

Now write $H = H_1 \times H_2$ where H_1 is the unique Sylow q-subgroup of H. Since $L \neq K$, the induction hypothesis shows that $L \leq H^g = H_1^g \times H_2^g$ for some $g \in G$. Thus $L \leq H_2^g$ because L is a q'-group. Consequently $N = N_G(L)$ contains $\langle H_1^g, K\rangle$. Observe that $|G : H_1|$ is not divisible by q; hence H_1^g is a Sylow q-subgroup of N and by Sylow's Theorem $Q \leq (H_1^g)^x$ for some $x \in N$. But $L = L^x$ and, using $L \leq H_2^g$, we obtain

$$K = QL = QL^x \leq H_1^{gx}H_2^{gx} = H^{gx},$$

as required. □

Exercises 9.1

1. Let G be a Frobenius group with kernel K. Prove that every complement of K in G is a Frobenius complement and that all Frobenius complements of K are conjugate in G (see Exercise 8.5.6).

*2. Let $N \lhd G$ and suppose that $|G : N| = m$ is finite and N is an abelian group in which every element is uniquely expressible as an mth power. Prove that N has a complement in G and all such complements are conjugate. [*Hint*: See the proof of 9.1.2.]

3. Let G be a countable locally finite group (i.e., finitely generated subgroups are finite). Suppose that $N \lhd G$ and that elements of N and G/N have coprime orders. Prove that N has a complement in G. Show also that not all the complements need be conjugate by considering the direct product of a countable infinity of copies of S_3.

4. If H is a subnormal subgroup of a group G, prove that $O_\pi(H) = H \cap O_\pi(G)$.

5. Let H and K be π-separable subgroups of a finite group G. If H is subnormal in G, prove that $\langle H, K\rangle$ is π-separable.

6. If p divides the order of a finite soluble group G, prove that there is a maximal subgroup whose index is a power of p. Show that this is false for insoluble groups.

7. Let G be a finite soluble group whose order has exactly k prime divisors where $k > 1$. Prove that there is a prime p and a Hall p'-subgroup H such that $|G| \leq |H|^{k/k-1}$. [*Hint*: Let $|G| = p_1^{e_1} \cdots p_k^{e_k}$ and consider the smallest $p_i^{e_i}$.]

8. Let G be a finite soluble group whose order has at least three distinct prime divisors. If every Hall p'-subgroup of G is nilpotent, show that G is nilpotent. [*Hint*: Prove that each Sylow subgroup is normal.]

9. (Wielandt). If a finite group G has three soluble subgroups H_1, H_2, H_3 with their indices coprime in pairs, then G is soluble. [*Hint*: Use induction on the order of G. Assume $H_1 \neq 1$ and choose a minimal normal subgroup N of H_1: show that N^G is contained in either H_2 or H_3.]

10. A finite group in which every subgroup is either subnormal or nilpotent is soluble. [Use 9.1.9.]

11. Let $G = PQ$ be a finite minimal nonnilpotent group with the notation of 9.1.9. Derive the following information about G:
    (a) Frat $Q \leq \zeta G$.
    (b) $P = [P, Q]$ and Frat $P \leq \zeta(G)$, so P is nilpotent of class at most 2.
    (c) If p is odd, $P^p = 1$, while $P^4 = 1$ if $p = 2$ [*Hint*: Prove that $[a, x]^p = 1$ or $[a, x]^4 = 1$ where $a \in P$ and $x \in Q$.]

12. (Itô). Let G be a group of odd order. If every minimal subgroup lies in the center, prove that G is nilpotent. [Use Exercise 9.1.11.]

13. (Itô). Let G be a group of odd order. If every minimal subgroup of G' is normal in G, prove that G' is nilpotent and G is soluble.

*14. Let N be a minimal normal subgroup of a finite soluble group G such that $N = C_G(N)$. Prove that N has a complement in G and all such complements are conjugate. [*Hint*: Let L/N be minimal normal in G/N. Show that N has a complement X in L and argue that $N_G(X)$ is a complement of N in G.]

9.2. Sylow Systems and System Normalizers

Let G be a finite group and let $p_1, \dots, p_k$ denote the distinct prime divisors of $|G|$. Suppose that Q_i is a Hall p_i'-subgroup of G. Then the set $\{Q_1, \dots, Q_k\}$ is called a *Sylow system* of G. It is a direct consequence of 9.1.7 and 9.1.8 that *a finite group has a Sylow system if and only if it is soluble.*

A Sylow system determines a set of permutable Sylow subgroups of G in the following manner.

9.2.1. *Let $\{Q_1, \dots, Q_k\}$ be a Sylow system of the finite soluble group G.*

(i) *If π is any set of primes, then $\bigcap_{p_i \notin \pi} Q_i$ is a Hall π-subgroup of G. In particular $P_i = \bigcap_{j \neq i} Q_j$ is a Sylow p_i-subgroup of G.*
(ii) *The Sylow subgroups $P_1, \dots, P_k$ are permutable in pairs, that is, $P_iP_j = P_jP_i$.*

Proof. Let $|G| = p_1^{e_1} \cdots p_k^{e_k}$ where $|G : Q_i| = p_i^{e_i}$. It follows from 1.3.11 that $H = \bigcap_{p_i \notin \pi} Q_i$ has index equal to $\prod_{p_i \notin \pi} p_i^{e_i}$, which shows that H is a Hall π-subgroup of G. Applying this result to $\pi = \{p_i, p_j\}$, $i \neq j$, we conclude that $K = \bigcap_{k \neq i,j} Q_k$ is a Hall π-subgroup with order $p_i^{e_i}p_j^{e_j}$, containing P_i and P_j. Since $|P_iP_j| = p_i^{e_i}p_j^{e_j}$, it follows that $P_iP_j = K = P_jP_i$. □

A set of mutually permutable Sylow subgroups, one for each prime dividing the group order, is called a *Sylow basis*. By 9.2.1, if $\mathscr{Q} = \{Q_1, \dots, Q_k\}$ is a Sylow system of finite soluble group G, there is a corresponding *Sylow basis* $\mathscr{Q}^* = \{P_1, \dots, P_k\}$ given by $P_i = \bigcap_{j \neq i} Q_j$. In fact the converse holds: each Sylow basis determines a Sylow system.

9.2.2. *If G is a finite soluble group, the function $\mathscr{Q} \mapsto \mathscr{Q}^*$ is a bijection between the set of Sylow systems and the set of Sylow bases of G.*

Proof. Let $\mathscr{P} = \{P_1, \ldots, P_k\}$ be any Sylow basis of G and define $Q_i = \prod_{j \neq i} P_j$. Since the P_j are permutable, Q_i is a subgroup. From its order we can tell that Q_i is a Hall p_i'-subgroup. Hence $\mathscr{P}_* = \{Q_1, \ldots, Q_k\}$ is a Sylow system of G. Finally one easily verifies that

$$\bigcap_{i \neq k} \prod_{j \neq i} P_j = P_k \qquad \text{and} \qquad \prod_{k \neq i} \bigcap_{j \neq k} Q_j = Q_i,$$

so that $\mathscr{P} \mapsto \mathscr{P}_*$ and $\mathscr{Q} \mapsto \mathscr{Q}^*$ are inverse mappings. □

Two Sylow systems $\{Q_1, \ldots, Q_k\}$ and $\{\bar{Q}_1, \ldots, \bar{Q}_k\}$ of G are said to be *conjugate* if there is an element g of G such that $Q_i^g = \bar{Q}_i$ for $i = 1, 2, \ldots, k$. Conjugacy of two Sylow bases is defined in the same way.

9.2.3 (P. Hall). *In a finite soluble group G any two Sylow systems are conjugate, as are any two Sylow bases.*

Proof. Denote by $\mathscr{S}_i$ the set of all Hall p_i'-subgroups of G. Then G acts on $\mathscr{S}_i$ by conjugation and 9.1.7 shows that this action is transitive. Consequently $|\mathscr{S}_i| = |G : N_G(Q_i)|$ where $Q_i \in \mathscr{S}_i$: it follows that $|\mathscr{S}_i|$ divides $|G : Q_i|$ and equals a power of p_i. Now G also acts by conjugation on the set $\mathscr{S} = \mathscr{S}_1 \times \cdots \times \mathscr{S}_k$ of all Sylow systems. An element of G fixes $(Q_1, \ldots, Q_k)$ if and only if it normalizes each Q_i. Thus the stabilizer of $(Q_1, \ldots, Q_k)$ in G is the intersection of all the $N_G(Q_i)$, which has index equal to $\prod_{i=1}^k |\mathscr{S}_i| = |\mathscr{S}|$. But this means that G acts transitively on $\mathscr{S}$, which is just to say that any two Sylow systems are conjugate. Applying the mapping $\mathscr{Q} \mapsto \mathscr{Q}^*$ and using 9.2.2 we deduce the corresponding result for Sylow bases. □

System Normalizers

Let $\{Q_1, \ldots, Q_k\}$ be a Sylow system of a finite soluble group G. The subgroup

$$N = \bigcap_{i=1}^{k} N_G(Q_i)$$

is called a *system normalizer* of G. We shall see that these subgroups have many remarkable properties. Notice that if $\{P_1, \ldots, P_k\}$ is the corresponding Sylow basis, an element of G normalizes every Q_i if and only if it normalizes every P_i: this in on account of the relation between the P_i and the Q_i (see 9.2.1 and 9.2.2). Hence

$$N = \bigcap_{i=1}^{k} N_G(P_i).$$

and the system normalizers can also be obtained from Sylow bases.

9.2.4. *In a finite soluble group the system normalizers are nilpotent and any two are conjugate.*

Proof. Let $\{P_1, \dots, P_k\}$ be a Sylow basis giving rise to a system normalizer N. Now $|N : N \cap P_i| = |NP_i : P_i|$ divides $|G : P_i|$ since $P_i \lhd NP_i$. Hence $N \cap P_i$ is a Sylow p_i-subgroup of N. Also $N \cap P_i \lhd N$. It follows from 5.2.4 that N is nilpotent. The conjugacy of the system normalizers is a direct consequence of the conjugacy of the Sylow systems. □

Covering and Avoidance

Suppose that G is a group and let $K \lhd H \leq G$ and $L \leq G$. Then L is said to *cover* H/K if $HL = KL$, or equivalently, if $H = K(H \cap L)$. On the other hand, if $H \cap L = K \cap L$, that is, if $H \cap L \leq K$, then L is said to *avoid* H/K.

9.2.5. *Let G be a finite soluble group and let H/K be a principal factor of G which is a p-group. Let $M \lhd G$ and denote by Q a Hall p'-subgroup of M. Then $N_G(Q)$ covers or avoids H/K according as M centralizes H/K or not.*

Proof. Denote $N_G(Q)$ by L. First of all suppose that M centralizes H/K, so that $[H, M] \leq K$. Now $Q^H = Q[H, Q]$ by 5.1.6 and, because $Q \leq M$, it follows that $Q^H \leq Q(K \cap M)$. If $x \in H$, then Q and Q^x are clearly Hall p'-subgroups of $Q(K \cap M)$ and 9.1.7 shows that they are conjugate, say $Q^x = Q^y$ for some y in $K \cap M$. Hence $xy^{-1} \in L$ and $x \in LK = KL$, which shows that L covers H/K.

Now suppose that M does not centralize H/K and write $C = C_G(H/K)$; then $D \equiv C \cap M < M$ and consequently there is a principal factor E/D of G such that $E \leq M$; thus $E \nleq C$. Now E/D acts via conjugation on H/K. If E/D were a p-group, the natural semidirect product $(E/D) \ltimes (H/K)$ would be a finite p-group and hence nilpotent, which would imply that $[H, E]K < H$ and thus $[H, E] \leq K$: however this is false because $E \nleq C$. Therefore the principal factor E/D is a p'-group, from which we deduce that $E \leq DQ$: for Q is a Hall p'-subgroup of M. It follows that

$$[H \cap L, E] \leq [H \cap L, DQ] \leq [H \cap L, D][H \cap L, Q] \leq K;$$

for $D \leq C$, while $[H \cap L, Q] \leq H \cap L \cap Q \leq K$ since H/K is a p-group. Thus $(H \cap L)K/K \leq C_{H/K}(EK/K)$; now the latter is G-admissible and not equal to H/K because $E \nleq C$. Since H/K is a principal factor, $C_{H/K}(EK/K)$ is trivial, so $H \cap L \leq K$ and L avoids H/K. □

This result is the stepping stone to a fundamental covering and avoidance property of system normalizers.

9.2.6 (P. Hall). *If N is a system normalizer of a finite soluble group G, then N covers the central principal factors and avoids the noncentral principal factors of G.*

Proof. Let $1 = G_0 < G_1 < \cdots < G_n = G$ be a principal series of G. Let the system normalizer N arise from a Sylow system $\{Q_1, \dots, Q_k\}$ and put $N_i = N_G(Q_i)$, so that $N = N_1 \cap \cdots \cap N_k$.

According to 9.2.5 (with G in place of M), the subgroup N_i covers the central p_i-principal factors and avoids the noncentral p_i-principal factors (here Q_i is a Hall p_i'-subgroup). Hence N certainly avoids the noncentral principal factors. Now $|G_{j+1}N_i : G_jN_i|$ equals 1 or $|G_{j+1} : G_j|$ according to whether N_i covers or avoids G_{j+1}/G_j. It follows that $|G : N_i|$ equals the product of the orders of the noncentral p_i-principal factors. Since the $|G : N_i|$ are relatively prime, $|G : N|$ equals the product of the orders of all the noncentral principal factors. This implies that $|N|$ equals the product of the orders of the central principal factors. But $|N|$ equals the product of all the indices $|G_{j+1} \cap N : G_j \cap N|$ where G_{j+1}/G_j is central; for N avoids noncentral factors. Hence $|G_{j+1} \cap N : G_j \cap N| = |G_{j+1} : G_j|$ if G_{j+1}/G_j is central: this implies that $G_{j+1} = G_j(G_{j+1} \cap N)$ and N covers G_{j+1}/G_j. □

An interesting corollary of 9.2.6 is the fact that *the order of a system normalizer equals the product of the orders of all the central factors in a principal series.*

As an application of the covering-avoidance property of system normalizers, we shall prove a theorem on the existence of complements.

9.2.7 (Gaschütz, Schenkman, Carter). *Let G be a finite soluble group and denote by L the smallest term of the lower central series of G. If N is any system normalizer in G, then $G = NL$. If in addition L is abelian, then also $N \cap L = 1$ and N is a complement of L.*

Proof. Form a principal series of G through L by refining $1 \lhd L \lhd G$. Since G/L is nilpotent, principal factors "above" L will be central and hence are covered by N (by 9.2.6). Therefore $G = NL$.

Now assume that L is a abelian. Then it is sufficient to prove that no principal factor of G "below" L is central: for by 9.2.6 the system normalizer N will avoid such factors and $N \cap L$ will be trivial. We shall accomplish this by induction on $|L| > 1$. By the induction hypothesis it suffices to show that $L \cap \zeta G = 1$.

If $C = C_G(L)$, then $L \leq C < G$ since $L = [L, G] \neq 1$. Hence G/C is nilpotent; we now choose a nontrivial element gC from the center of G/C, noting that $[L, [g, G]] = 1$. We deduce from this relation and one of the fundamental commutator identities that if $a \in L$ and $x \in G$, then

$$[a, g]^x = [a^x, g^x] = [a^x, [x, g^{-1}]g] = [a^x, g].$$

Hence the mapping $\theta: L \to L$ defined by $a^\theta = [a, g]$ is a nonzero G-endomorphism of L, and $\operatorname{Ker}\theta \lhd G$. Since $L \cap \zeta G \leq \operatorname{Ker}\theta$, we may assume $\operatorname{Ker}\theta \neq 1$, so that $(L/\operatorname{Ker}\theta) \cap \zeta(G/\operatorname{Ker}\theta)$ is trivial by induction. Also $L/\operatorname{Ker}\theta \simeq^G L^\theta$, from which it follows that $L^\theta \cap \zeta G = 1$. Now $1 \neq L^\theta \lhd G$ and $(L/L^\theta) \cap \zeta(G/L^\theta)$ is trivial by induction. Therefore $L \cap \zeta G = 1$, as required. □

9.2.8. *Let N be a system normalizer of a finite soluble group G. Then N_G, the core of N in G, equals the hypercenter of G and the normal closure of N equals G itself.*

Proof. Let H be the hypercenter of G and refine the series $1 \lhd H \lhd G$ to a principal series. By 9.2.6 every central principal factor is covered by N, so $H \leq N$ and hence $H \leq N_G = K$, say. If $H \neq K$, there is a principal factor L/H where $L \leq K$. Now since L/H cannot be central, it is avoided by N. But $L \leq K \leq N$, from which it follows that $L = H$, a contradiction.

If the normal closure N^G were proper, it would lie inside a maximal normal subgroup of G, say M. But G/M is abelian since G is soluble. Hence N covers G/M and $G = MN = M$, which cannot be true. □

Since N^G is generated by conjugates of N, we deduce from 9.2.8 the following fact.

9.2.9. *A finite soluble group is generated by its system normalizers.*

Abnormal Subgroups

A subgroup H of a group G is called *abnormal* if $g \in \langle H, H^g \rangle$ for all g in G. For example, it is simple to show that a nonnormal maximal subgroup is always abnormal. Abnormality is a strong form of nonnormality which leads to an interesting characterization of system normalizers.

Important examples of abnormal subgroups are the Sylow normalizers.

9.2.10. *Let N be a normal subgroup of the finite group G and let P be a Sylow p-subgroup of N. Then $N_G(P)$ is abnormal in G.*

Proof. Let $H = N_G(P)$ and put $K = \langle H, H^g \rangle$ where g is some element of G. Now P and P^g are conjugate in $K \cap N$ since they are Sylow p-subgroups of that group. Therefore $P^g = P^x$ for some x in $K \cap N$, and $gx^{-1} \in H$. It follows that $g \in K$, as requred. □

An abnormal subgroup H always coincides with its normalizer: for if $g \in N_G(H)$, then $g \in \langle H, H^g \rangle = H$. Now it is obvious that any subgroup of G that contains an abnormal subgroup is itself abnormal. Consequently every

subgroup that contains H is also self-normalizing. In fact the converse of this statement is true for finite soluble groups.

9.2.11 (Taunt). *Let G be a finite soluble group and let H be a subgroup. Then H is abnormal in G if and only if every subgroup containing H coincides with its normalizer in G.*

For the proof we require a simple lemma.

9.2.12. *Let G be a finite group and let $H \leq G$ and $N \lhd G$. If H is abnormal in HN and HN is abnormal in G, then H is abnormal in G.*

Proof. If $g \in G$, then $g \in \langle HN, (HN)^g \rangle = N\langle H, H^g \rangle$; thus $g = xy$ where $x \in N$ and $y \in \langle H, H^g \rangle$. Now $x \in \langle H, H^x \rangle$ since H is abnormal in HN. Hence $x \in \langle H, H^{gy^{-1}} \rangle \leq \langle H, H^g \rangle$ since $y \in \langle H, H^g \rangle$. Finally $g \in \langle H, H^g \rangle$ as required. □

***Proof of* 9.2.11.** Only the sufficiency of the condition is in question: assume that H satisfies the condition. We shall prove that H is abnormal in G by induction on $|G| > 1$. If N is a minimal normal subgroup of G, the hypothesis on H is inherited by HN/N, with the result that HN/N is abnormal in G/N by induction. Obviously this means that HN is abnormal in G. If $HN \neq G$, then H is abnormal in HN, by induction once again, and the desired conclusion follows from 9.2.12. Finally, suppose that $HN = G$. Then, since N is abelian, $H \cap N = 1$; we may apply 5.4.2 to show that H is maximal in G. However $H = N_G(H)$ by hypothesis, so H is abnormal in G. □

System Normalizers and Abnormality

The aim of the rest of this section is to explore the relationship between abnormality and system normalizers, the principal theorem (9.2.15) being a characterization of system normalizers. For the latter we shall need two preliminary results.

9.2.13. *Let M be a nonnormal maximal subgroup of a finite soluble group G and let $|G:M| = p^m$. If Q is a Hall p'-subgroup of M, then $N_G(Q) \leq M$.*

Proof. In the first place $|G:M|$ is indeed a power of a prime p by 5.4.3. Induct on $|G| > 1$. If the core of M in G—call it K—is nontrivial, then $N_{G/K}(QK/K) \leq M/K$ by induction, which surely implies that $N_G(Q) \leq M$. Henceforth we suppose that $K = 1$. Choose a minimal normal subgroup N of G; then $N \nleq M$, so that $G = MN$ and $M \cap N \lhd G$. (Keep in mind that N must be abelian because G is soluble.) It follows that $M \cap N = 1$ and $|N| = |G:M| = p^m$.

Let N_1 be minimal normal in M and suppose that N_1 is a p-group. Then NN_1 is a p-group and hence is nilpotent; thus $[N, N_1] < N$. But $[N, N_1] \lhd MN = G$, so $[N, N_1] = 1$ and $1 \neq N_1 \lhd MN = G$. However, since M has trivial core, this is impossible. It follows that N_1 has order prime to p and in consequence $N_1 \leq Q$. Writing L for $N_G(Q)$, we argue that $N_1^L \leq N_1^{MN} = N_1^N \leq N_1 N$. Therefore $N_1^L \leq (N_1 N) \cap Q = N_1$ and $L \leq N_G(N_1)$. The latter subgroup equals M since $N_1 \lhd M$ and M is maximal: thus $L \leq M$. □

9.2.14. *If M is a nonnormal maximal subgroup of a finite soluble group G, then every system normalizer of M contains a system normalizer of G.*

Proof. Let $\{Q_1, \dots, Q_k\}$ be a Sylow system of G where Q_i is a Hall p_i'-subgroup of G. The index of M is G is a prime power, say p_1^m. Since a Hall p_1'-subgroup of M is also a Hall p_1'-subgroup of G, we may assume that $Q_1 \leq M$. If $i > 1$, the indices $|G : M|$ and $|G : Q_i|$ are relatively prime and we conclude from Exercise 1.3.8 that $G = MQ_i$. Hence $|M : M \cap Q_i| = |G : Q_i|$, which is a power of p_i. It follows that $M \cap Q_i$ is a Hall p_i'-subgroup of M and that $\{Q_1 = M \cap Q_1,\ M \cap Q_2, \dots, M \cap Q_k\}$ is a Sylow system of M. Since $N_G(Q_1) \leq M$ by 9.2.13,

$$\bigcap_{i=1}^{k} N_G(Q_i) = \bigcap_{i=1}^{k} N_M(Q_i) \leq \bigcap_{i=1}^{k} N_M(M \cap Q_i).$$

Hence some system normalizer of G is contained in one of M. The required result follows from the conjugacy of the system normalizers of M. □

Subabnormal Subgroups

A subgroup H of a group G is said to be *subabnormal* in G if there is a finite chain of subgroups $H = H_0 < H_1 < \cdots < H_n = G$ such that H_i is abnormal in H_{i+1}. Subabnormality is a weaker property than abnormality. Our interest in subabnormality stems from the next theorem.

9.2.15 (P. Hall). *The system normalizers of a finite soluble group G are precisely the minimal subabnormal subgroups of G.*

Proof. Firstly it will be established that every subabnormal subgroup H contains a system normalizer of G. By definition there is a chain $H = H_0 < H_1 < \cdots < H_s = G$ such that H_i is abnormal in H_{i+1}. Since additional terms can be inserted in the chain without disturbing abnormality, we may assume that H_i is maximal in H_{i+1}. Of course H_i is not normal in H_{i+1}. Thus 9.2.14 implies that each system normalizer of H_i contains one of H_{i+1}, and surely H contains a system normalizer of G.

To complete the proof it is sufficient to prove that every system normalizer is subabnormal. If G is nilpotent, the only system normalizer is G itself:

for this reason we shall suppose that G is not nilpotent. Choose a principal series of G and let H be the smallest nonnilpotent term in the series. If K is the preceding term, then K is nilpotent and, of course, H/K is a principal factor of G with order p^k, say, where p is prime. If P is a Sylow p-subgroup of H, then $H = PK$ and P cannot be normal in H; otherwise the latter would be nilpotent in view of 5.2.8. Thus $L = N_G(P) \neq G$; note that L is abnormal in G by 9.2.10. Also the Frattini argument (5.2.14) implies that $G = LH = LPK = LK$.

We show next that any system normalizer N of L is automatically a system normalizer of G. By induction on $|G|$ we have that N is subabnormal in L and hence in G. Applying the result of the first paragraph, we conclude that N contains a system normalizer of G. Since system normalizers of G, being conjugate, have the same order, it suffices to prove that N is contained in a system normalizer of G.

Let N arise from the Sylow system $\{Q_1, \dots, Q_k\}$ of L. Writing K_i for the unique Hall p_i'-subgroup of the nilpotent group K, we observe that $K_i \lhd G$ and $Q_i^* \equiv Q_i K_i$ is a p_i'-group. Also $|G : Q_i^*| = |LK : Q_i K_i|$ is a power of p_i since both $|L : Q_i|$ and $|K : K_i|$ are powers of p_i. Therefore Q_i^* is a Hall p_i'-subgroup of G and $\{Q_1^*, \dots, Q_k^*\}$ is a Sylow system of G—with corresponding system normalizer N^*, let us say. Since $N_L(Q_i) \leq N_G(Q_i^*)$, we obtain $N \leq N^*$ as required.

Finally, N is subabnormal in L, which is abnormal in G; hence N is subabnormal in G. This completes the proof since all system normalizers of G are conjugate. □

Exercises 9.2

1. Locate the system normalizers of the groups S_3, A_4, S_4, SL(2, 3).

2. Let G be a finite soluble group and let π be the set of prime divisors of $|G|$. Let $\pi = \pi_1 \cup \pi_2 \cup \cdots \cup \pi_k$ be any partition of π. Prove that there exists a set of pairwise permutable Hall π_i-subgroups, $i = 1, 2, \dots, k$.

3. (P. Hall). Let G be a finite soluble group of order $\prod_{i=1}^{k} p_i^{e_i}$, where the p_i are distinct primes. Prove that the order of Out G divides the number $\prod_{i=1}^{k} m_i p_i^{d_i(e_i - d_i)}$, where $m_i = |\mathrm{GL}(d_i, p_i)|$ and d_i is the minimal number of generators of a Sylow p_i-subgroup of G. [*Hint*: Let $\mathscr{S}$ be a Sylow basis of G and let $\gamma \in \mathrm{Aut}\, G$: now consider $\mathscr{S}^\gamma$.]

4. Show that the last part of 9.2.7 need not be true if L is nonabelian.

5. Let G be a finite soluble group in which the last term L of the lower central series is abelian. Prove that every complement of L is a system normalizer.

6. Give an example of a subabnormal subgroup that is not abnormal.

7. Let G be a finite soluble group which is not nilpotent but all of whose proper quotients are nilpotent. Denote by L the last term of the lower central series. Prove the following statements:

(a) L is minimal normal in G;
(b) L is an elementary abelian p-group;
(c) there is a complement $X \neq 1$ of L which acts faithfully on L;
(d) the order of X is not divisible by p.

8. Suppose that $X \neq 1$ is a finite nilpotent p'-group that acts faithfully on a simple FX-module L where $F = \mathrm{GF}(p)$. Prove that every proper quotient of $G = X \ltimes L$ is nilpotent but G is not nilpotent.

9. Let G be a finite soluble group which is not abelian but all of whose proper quotients are abelian. Prove that either G is generalized extra-special (see Exercise 5.3.8) or G is isomorphic with a subgroup of $H(q)$ where $q > 2$ (see 7.1).

9.3. p-Soluble Groups

If π is a set of primes, a finite group G is called *π-soluble* if it has a series whose factors are π-groups or π'-groups and if the π-factors are soluble. Equivalently we could have said that each composition factor is either a π-group or a π'-group and in the former case has prime order. (The reader should supply a proof.) π-solubility is, therefore, a strong form of π-separability. Evidently all finite soluble groups are π-soluble. Of particular importance is *p-solubility* (which is the same as p-separability), a concept introduced in 1956 by P. Hall and G. Higman [a80] in a paper of great significance for finite group theory.

The following result is basic.

9.3.1. *If G is a π-separable group, then $C_G(O_{\pi'\pi}(G)/O_{\pi'}(G)) \leq O_{\pi'\pi}(G)$.*

Proof. Clearly we can assume that $O_{\pi'}(G) = 1$ and prove that $C_G(O_\pi(G)) \leq O_\pi(G)$. Put $P = O_\pi(G)$ and $C = C_G(P)$. Then $P \cap C = \zeta P \lhd G$, so that $\zeta P \leq O_\pi(C)$. Also $O_\pi(C) \leq P \cap C = \zeta P$, and it follows that $\zeta P = O_\pi(C)$. If $C \nleq P$, then $O_\pi(C) = \zeta P < C$. Since C is π-separable, there exists a characteristic subgroup L of C such that $O_\pi(C) < L$ and $L/O_\pi(C)$ is a π'-group. By the Schur–Zassenhaus Theorem (9.1.2) there is a subgroup K such that $L = K(O_\pi(C))$ and $K \cap O_\pi(C) = 1$. In fact $L = K \times O_\pi(C)$ because $K \leq C$ and C centralizes $O_\pi(G)$. It follows that K is normal in G, being the unique Sylow π'-subgroup of L. Thus $K \leq O_{\pi'}(G) = 1$ and $L = O_\pi(C)$, in contradiction to the choice of L. □

9.3.2 (Hall–Higman). *Let G be a p-soluble group such that $O_{p'}(G) = 1$. If P denotes $O_p(G)$, then conjugation leads to a faithful representation of G/P as a group of linear transformations of the vector space $P/\mathrm{Frat}\, P$.*

Proof. Recall that $\mathrm{Frat}\, P = P'P^p$ by 5.3.2, so that $P/\mathrm{Frat}\, P$ is a vector space over $\mathbb{Z}_p$. Thus $C = C_G(P/\mathrm{Frat}\, P)$ contains P. If $D = C_G(P)$, then $D \leq C$ and C/D is a p-group by 5.3.3. Also $D \leq O_p(G)$ by 9.3.1, so C is a p-group. Since $C \lhd G$, it follows that $C = P$. □

p-Nilpotent Groups

A finite group G is said to be *p-nilpotent* (where p is a prime) if it has a normal Hall p'-subgroup, that is, if $O_{p'p}(G) = G$. Obviously every finite nilpotent group is p-nilpotent; conversely a finite group which is p-nilpotent for all p is nilpotent, as the reader should check.

The product of all the normal p-nilpotent subgroups of a finite group is clearly $O_{p'p}(G)$: this is the maximum normal p-nilpotent subgroup of G and we shall also write it

$$\mathrm{Fit}_p(G),$$

the *p-Fitting subgroup.*

The following characterization of $\mathrm{Fit}_p(G)$ is analogous to an already proven characterization of Fit G—see 5.2.9.

9.3.3. *If G is a finite group, then* $\mathrm{Fit}_p(G)$ *equals the intersection of the centralizers of the principal factors of G whose orders are divisible by p.*

Proof. Let H be a normal p-nilpotent subgroup of G and let N be a minimal normal subgroup of G whose order is divisible by p. Assume that $[H, N] \neq 1$. Then $H \cap N \neq 1$ and thus $N \leq H$. Now $N \nleq O_{p'}(H)$, so that $N \cap O_{p'}(H) = 1$. Hence N is a p-group. Also $C_H(N) \geq O_{p'}(H)$ and $\bar{H} = H/C_H(N)$ is a p-group. The natural semidirect product $\bar{H} \ltimes N$ is a p-group, so it is nilpotent and $[H, N] < N$. This implies that $[H, N] = 1$ since N is minimal normal in G. It follows by induction on $|G|$ that H centralizes every principal factor whose order is divisible by p.

Now let C be the intersection of the centralizers of the principal factors whose orders are divisible by p. Then $\mathrm{Fit}_p(G) \leq C$ by the previous paragraph. We are required to prove that C is p-nilpotent. Let N be minimal normal in G. Then by induction on the group order $CN/N \simeq C/C \cap N$ is p-nilpotent. We may therefore assume that $C \cap N \neq 1$, so that $N \leq C$ and C/N is p-nilpotent. If N is a p'-group, it is obvious that C is p-nilpotent. Suppose that p divides $|N|$; then $[N, C] = 1$ and $N \leq \zeta C$. It follows that N is a p-group. Let $M/N = O_{p'}(C/N)$: clearly C/M is a p-group. Because $N \leq \zeta M$ we can apply 9.1.2 to show that M has a normal Hall p'-subgroup L. But C/L is a p-group, so C is p-nilpotent. □

Another analogue of a result on nilpotency is next (see 5.2.15).

9.3.4. *Let G be a finite group and assume that* Frat $G \leq N \lhd G$ *and* $N/\mathrm{Frat}\ G$ *is p-nilpotent. Then N is p-nilpotent. Hence* $\mathrm{Fit}_p(G/\mathrm{Frat}\ G) = \mathrm{Fit}_p(G)/\mathrm{Frat}\ G$.

Proof. Let $F = \mathrm{Frat}\ G$ and write $O_{p'}(N/F) = Q/F$. Since $O_{p'}(F)$ can be factored out if necessary, we may assume that F is a p-group. By 9.1.2 there is a subgroup H such that $Q = HF$ and $H \cap F = 1$: here of course H is a p'-group. If $g \in G$, then H and H^g are conjugate in Q, by 9.1.2 again: hence

$H^g = H^x$ for some x in Q and $gx^{-1} \in L = N_G(H)$. It follows that $G = LQ = LF$. However F consists of nongenerators by 5.2.12. Consequently $G = L$ and $H \lhd G$. Since N/H is obviously a p-group, N is p-nilpotent. □

In Chapter 10 we shall establish important criteria for a group to be p-nilpotent due to Frobenius and Thompson.

The p-Length of a p-Soluble Group

Recall that if G is a p-soluble group, the p-length $l_p(G)$ is the length of the upper $p'p$-series. We wish to relate this invariant to other invariants of G such as the nilpotent class of the Sylow p-subgroups. To begin with two simple lemmas will be established.

9.3.5. *If G is a finite group and p is a prime dividing $|G|$, then p also divides $|G : \text{Frat } G|$.*

Proof. Assume that $|G : \text{Frat } G|$ is not divisible by p; then a Sylow p-subgroup P of G is contained in Frat G. Since the latter is nilpotent, $P \lhd G$. By 9.1.2 there is a subgroup H such that $G = HP$ and $H \cap P = 1$. But, since $P \leq \text{Frat } G$, it follows that $G = H$ and $P = 1$, which contradicts the fact that p divides $|G|$. □

9.3.6. *If G is a p-soluble group, $l_p(G) = l_p(G/\text{Frat } G)$.*

Proof. If F denotes Frat G, then it is obvious that $l_p(G/F) \leq l_p(G)$. If $l_p(G/F) = 0$, then p does not divide $|G : F|$ and 9.3.5 shows that p cannot divide $|G|$: hence $l_p(G) = 0$. Suppose that $l_p(G/F) > 0$: now $\text{Fit}_p(G/F) = \text{Fit}_p(G)/F$ by 9.3.4, that is, $O_{p'p}(G/F) = O_{p'p}(G)/F \neq 1$. From this it follows that the upper $p'p$-series of G and G/F have same length. □

The fundamental theorem on p-length can now be established.

9.3.7 (Hall–Higman). *Let G be a p-soluble group.*

(i) *$l_p(G) \leq c_p(G)$ where $c_p(G)$ is the nilpotent class of a Sylow p-subgroup.*
(ii) *$l_p(G) \leq d_p(G)$ where $d_p(G)$ is the minimum number of generators of a Sylow p-subgroup.*
(iii) *$l_p(G) \leq s_p(G)$ where $s_p(G)$ is the maximum rank of a p-principal factor of G.*

Proof. (i) If $c_p(G) = 0$, then of course G is a p'-group and $l_p(G) = 0$: suppose that $c_p(G) > 0$ and proceed by induction on $c_p(G)$. Let P be a Sylow p-subgroup of G. Then $PO_{p'}(G)/O_{p'}(G)$ is a Sylow p-subgroup of $G/O_{p'}(G)$,

so it contains $O_{p'p}(G)/O_{p'}(G)$. Therefore ζP centralizes $O_{p'p}(G)/O_{p'}(G)$ and 9.3.1 shows that $\zeta P \leq O_{p'p}(G)$. From this it follows that $c_p(G/O_{p'p}(G)) \leq c_p(G) - 1$; consequently $l_p(G/O_{p'p}(G)) \leq c_p(G) - 1$. Finally

$$l_p(G) = l_p(G/O_{p'p}(G)) + 1,$$

so the desired inequality follows.

(ii) The proof employs induction on $d = d_p(G)$. Notice that $d = 0$ is to be interpreted as $P = 1$, so that $l_p(G) = 0$ in this case. Let $l_p(G) > 0$. Evidently we may assume that $O_{p'}(G) = 1$. Let $P_1 = O_p(G)$; then $P_1 \leq P$.

Suppose that $P_1 \leq \text{Frat } P$. Then $P_1 \leq \text{Frat } G$ by 5.2.13, which leads to $l_p(G/\text{Frat } G) \leq l_p(G/P_1) = l_p(G) - 1$, in contradiction to 9.3.6. Therefore $P_1 \not\leq \text{Frat } P$.

By the Burnside Basis Theorem (5.3.2) d equals the minimum number of generators of $P/\text{Frat } P$, so this group has order p^d. Now $\text{Frat}(P/P_1)$ contains $(\text{Frat } P)P_1/P_1$. Thus the Frattini quotient group of P/P_1 is an image of $P/(\text{Frat } P)P_1$ and its order is at most p^{d-1}. Application of the induction hypothesis to G/P_1 yields $l_p(G/P_1) \leq d - 1$ and hence $l_p(G) \leq d$.

(iii) Let $s = s_p(G)$. If s were 0, then G would be a p'-group and $l \equiv l_p(G)$ would equal 0; therefore we assume $s > 0$. Let H/K be a p-principal factor of G; then H/K has order p^n where $n \leq s$. Now $G/C_G(H/K)$ is isomorphic with a subgroup of $\text{Aut}(H/K)$ and $\text{Aut}(H/K) \simeq \text{GL}(n, p)$ (see Exercise 1.5.11). The set of (upper) unitriangular matrices in $\text{GL}(n, p)$ is a Sylow p-subgroup and its nilpotent class is equal to $n - 1$ (Exercise 5.1.11): it follows that $\gamma_n P$ centralizes H/K. Therefore $\gamma_s P$ centralizes every p-principal factor and $\gamma_s P \leq \text{Fit}_p(G) = O_{p'p}(G)$ by 9.3.3. By (i) we have

$$l_p(G/O_{p'p}(G)) \leq c_p(G/O_{p'p}(G)) \leq s - 1,$$

from which it follows immediately that $l_p(G) \leq s$. □

An application of 9.3.7 to the restricted Burnside Problem is given in 14.2.

p-Soluble Groups of p-Length at Most 1

A finite p-soluble group G has p-length at most 1 if and only if $O_{p'pp'}(G) = G$. For example, a p-nilpotent group has p-length ≤ 1. The next objective is a result of Huppert that characterizes soluble groups of p-length ≤ 1 in terms of their Sylow bases. This theorem is preceded by two preliminary results.

9.3.8. *Let G be a p-soluble group and suppose that every proper image of G has p-length $\leq k$ while $l_p(G) > k$. Then:*

(i) $\text{Frat}\, G = 1$;
(ii) $\text{Fit}_p(G) \equiv O_{p'p}(G) = N$ *is an elementary abelian p-group; this is also the unique minimal normal subgroup of* G;
(iii) $N = C_G(N)$ *and* N *has a complement in* G.

Proof. (i) follows at once from the equation $l_p(G/\text{Frat}\, G) = l_p(G)$ (see 9.3.6).

(ii) and (iii). Clearly $O_{p'}(G) = 1$, so N is a p-group. Also $\text{Frat}\, N \leq \text{Frat}\, G = 1$ by 5.2.13, which shows that N is elementary abelian. Now if N_1 and N_2 are nontrivial normal subgroups of G such that $N_1 \cap N_2 = 1$, then G/N_1 and G/N_2 both have p-length $\leq k$ and the mapping $g \mapsto (gN_1, gN_2)$ is a monomorphism of G into $G/N_1 \times G/N_2$; however this implies that $l_p(G) \leq k$. It follows that G has a unique minimal normal subgroup L and $L \leq N$. Since $\text{Frat}\, G = 1$, there is a maximal subgroup M which fails to contain L. Thus $G = ML$ and $M \cap L \lhd ML$ since L is abelian. Consequently $M \cap L = 1$ and M is a complement of L in G. Also $N = N \cap (ML) = (N \cap M)L$, and $N \cap M \lhd G$ since both M and L normalize $N \cap M$. If $N \cap M \neq 1$, then $L \leq N \cap M \leq M$, in contradiction to the choice of M. Therefore $N \cap M = 1$ and $N = L$.

Finally, suppose that $C = C_G(N)$ is strictly larger than N. Then $C = C \cap (MN) = (C \cap M)N$ and $1 \neq C \cap M \lhd G$. However this implies that $N \leq C \cap M$, which is impossible. □

It turns out that the property of having p-length at most 1 is closely connected with a curious permutability property of the Sylow p-subgroups of G. This is already indicated by the next result.

9.3.9. *Let G be a finite p-soluble group. Let P be a Sylow p-subgroup and Q a Hall p'-subgroup of G. If $P'Q = QP'$, then $l_p(G) \leq 1$.*

Proof. Let G be a counterexample to the assertion with least possible order. Since the hypothesis is inherited by images, every proper image of G has p-length ≤ 1. This is our opportunity to make use of 9.3.8. Thus $N = \text{Fit}_p(G)$ is a p-group and $N \leq P$. Therefore $N \cap (P'Q) = N \cap P' \lhd P$. But $N \cap (P'Q) \lhd P'Q$ and by examination of order $G = PQ$; hence $N \cap P' \lhd G$. Now, according to 9.3.8, the subgroup N is the unique minimal normal subgroup of G, so either $N \cap P' = 1$ or $N \leq P'$. In the first case $[N, P'] = 1$ because $N \leq P$; therefore $P' \leq C_G(N) = N$, by 9.3.8(iii). This leads to the successive conclusions $P' = 1$, $c_p(G) \leq 1$, and $l_p(G) \leq 1$ via 9.3.7. It follows that the other possibility $N \leq P'$ must prevail. Consequently $N \leq \text{Frat}\, P$. Applying 5.2.13(i) we conclude that $N \leq \text{Frat}\, G$. But $\text{Frat}\, G = 1$ by 9.3.8, so $N = 1$, a contradiction. □

We come now to the criterion referred to above.

9.3.10 (Huppert). *Let G be a finite soluble group and let $\{P_1, \ldots, P_k\}$ be a Sylow basis of G.*

(i) *If $P_i' P_j = P_j P_i'$ for all i and j, then $l_p(G) \leq 1$ for all p.*
(ii) *Conversely if $l_p(G) \leq 1$, every characteristic subgroup of P_i is permutable with every characteristic subgroup of P_j: in particular $P_i' P_j = P_j P_i'$.*

Proof. (i) Let Q_j be a Hall p_j'-subgroup arising from the given Sylow basis (as in 9.2.2); thus $Q_j = \prod_{k \neq j} P_k$. Hence P_j' surely permutes with Q_j by the hypothesis, and $l_p(G) \leq 1$ by 9.3.9.

(ii) Write $H = P_i P_j$, where $i \neq j$, keeping in mind that P_i and P_j permute since they belong to a Sylow basis. Clearly $l_p(H) \leq l_p(G) \leq 1$, which shows that the upper $p_j' p_j$-series of H has the form $1 \lhd N \lhd NP_j \lhd H$ where N and H/NP_j are p_j'-groups. Let K_j be characteristic in P_j. Since the natural homomorphism $P_j \to NP_j/N$ is an isomorphism, it follows that NK_j/N is characteristic in NP_j/N, and hence that $NK_j \lhd H$. Now $N \leq P_i$, so $P_i K_j = P_i(NK_j)$ is a subgroup. By 1.3.13 we deduce that $P_i K_j = K_j P_i = L$, say. Now $l_p(H) \leq 1$ and P_i and K_j are respectively a Sylow p_i- and a Sylow p_j-subgroup of L. If K_i is a characteristic subgroup of P_i, then $K_i K_j = K_j K_i$ by what has already been proved. □

EXERCISES 9.3

1. A finite group is nilpotent if and only if it is p-nilpotent for all p.
2. Give an example of a finite group that is p-nilpotent and q-nilpotent for two distinct prime divisors p, q of its order, but is not nilpotent.
3. A finite group is soluble if and only if it is p-soluble for all p.
4. A finite group is p-nilpotent if and only if every principal factor of order divisible by p is central.
5. A finite group is p-soluble of p-length ≤ 1 if and only if the group induces a p'-group of automorphisms in every principal factor whose order is divisible by p.
6. Let G be a finite p-soluble group with $O_{p'}(G) = 1$. Prove that $C_G(P/\text{Frat } P) = P$ where $P = O_p(G)$. Deduce that $|G|$ is bounded by a function of $|P|$.
7. Let G be a finite p-soluble group. Prove that G has an abelian Sylow p-subgroup if and only if $l_p(G) \leq 1$ and $O_{p'p}(G)/O_{p'}(G)$ is abelian.

9.4. Supersoluble Groups

During the exposition of basic properties of supersoluble groups in Chapter 5 it was shown that a maximal subgroup of a supersoluble group has prime index. Our object in this section is to prove that for finite groups the con-

verse of this statement is true, a result due to Huppert. We begin with an auxiliary result which is of independent interest.

9.4.1 (P. Hall). *If every maximal subgroup of a finite group G has index a prime or the square of a prime, then G is soluble.*

Proof. Let N be a minimal normal subgroup of G and denote by p the largest prime divisor of $|N|$. Let P be a Sylow p-subgroup of N and put $L = N_G(P)$. If $L = G$, then $P \lhd G$ and G/P is soluble by induction on $|G|$; hence G is soluble. Thus we may assume that $L < G$ and choose a maximal subgroup M which contains L. Then according to the hypothesis $|G:M| = q$ or q^2 for some prime q. By the Frattini argument $G = NL = NM$ and $|G:M| = |N:N \cap M|$, from which we deduce that q divides $|N|$ and consequently $q \leq p$.

Next, the conjugates of P in G account for all the Sylow p-subgroups of N; therefore $|G:L| \equiv 1 \bmod p$ by Sylow's Theorem. For the same reason $|M:L| \equiv 1 \bmod p$ and it follows that $|G:M| \equiv 1 \bmod p$. Now $q \not\equiv 1 \bmod p$ because $q \leq p$, so we are left with only one possibility, $|G:M| = q^2 \equiv 1 \bmod p$ and thus $q \equiv -1 \bmod p$. However this is possible only if $p = 3$ and $q = 2$. Thus $|N:N \cap M| = 4$ and consequently N has as an image some nontrivial subgroup of S_4 (see 1.6.6). Hence $N > N'$ and $N' = 1$ by minimality. Thus N is abelian, while G/N is soluble by induction. Finally, we conclude that G is soluble. □

We shall also need two results of a more elementary character.

9.4.2. *Let N be a minimal normal subgroup of the finite soluble group G and let $N \leq L \lhd G$. Assume that L/N is p-nilpotent but L is not. Then N has a complement in G.*

Proof. Suppose first that $N \leq \text{Frat}\, G = F$. Then LF/F is p-nilpotent. However, by 9.3.4 this implies that LF, and hence L, is p-nilpotent. Thus there exists a maximal subgroup M not containing N. Then $G = MN$ and $M \cap N \lhd G$ since N is abelian. Hence $M \cap N = 1$. □

9.4.3. *Let G be an irreducible abelian subgroup of* $\mathrm{GL}(n, p)$. *Then G is a cyclic group of order m where n is the smallest positive integer such that $p^n \equiv 1 \bmod m$.*

Proof. Let us identify G with a group of linear transformations of an n-dimensional vector space V over $F_p = \mathrm{GF}(p)$. Then V is a simple module over $R = F_pG$. Choose any nonzero vector v from V. Then $r \mapsto vr$ is an R-module homomorphism from R onto V, the kernel I being a maximal ideal since $R/I \simeq V$. Hence $F = R/I$ is a finite field of order p^n. Now the mapping $g \mapsto g + I$ is a monomorphism θ from G to F^*. Consequently G is cyclic.

Also $m = |G|$ divides $p^n - 1$ and $p^n \equiv 1 \bmod m$. Let n_1 be a smaller positive integer than n. Since the equation $t^{p^{n_1}} = t$ has only p^{n_1} solutions in F and since G^θ generates F, we must have $g^{p^{n_1}} \neq g$ for some g in G. Hence $p^{n_1} \not\equiv 1 \bmod m$. □

We come now to the principal theorem of this section.

9.4.4 (Huppert). *Let G be a finite group. If every maximal subgroup has prime index, then G is supersoluble.*

Proof. In the first place 9.4.1 assures us that G is at least soluble. We assume that $|G| > 1$ and employ induction on $|G|$. Let N be a minimal normal subgroup of G; then G/N is supersoluble by the induction hypothesis, and N is an elementary abelian p-group, say of order p^n. Our task is to prove that $n = 1$.

Let $L/N = O_{p'p}(G/N)$, so L/N is p-nilpotent. Assume that L is *not* p-nilpotent. Then by 9.4.2 there is a subgroup X such that $G = XN$ and $X \cap N = 1$. Thus $|G:X| = |N| = p^n$. But it is clear that X is maximal in G, whence it follows that $n = 1$.

Now assume that L *is* p-nilpotent. Consider a p-principal factor H/K of G such that $N \leq K$. Since G/N is supersoluble, $|H:K| = p$ and thus $G/C_G(H/K)$ is abelian with order dividing $p - 1$. If g is any element of G, then g^{p-1} centralizes every p-principal factor of G/N. Applying 9.3.3 we conclude that $g^{p-1} \in L$. Also $G' \leq L$ for the same reason, so G/L is abelian with order dividing $p - 1$.

Next $[N, L] \lhd G$, so either $N = [N, L]$ or $[N, L] = 1$; in the former event, since L is p-nilpotent and thus $L/O_{p'}(L)$ is nilpotent, we should have $N \leq O_{p'}(L)$ and $N = 1$. It follows that $[N, L] = 1$ and $L \leq C_G(N)$. Thus $\bar{G} = G/C_G(N)$ is abelian with exponent dividing $p - 1$. It is also isomorphic with an irreducible subgroup of $GL(n, p)$. We deduce from 9.4.3 that $\bar{G}$ is cyclic of order m where n is the smallest positive integer such that $p^n \equiv 1 \bmod m$. However m divides $p - 1$, so in fact $p \equiv 1 \bmod m$ and $n = 1$. □

Note the following consequence of Huppert's theorem.

9.4.5. *If G is a finite group and $G/\text{Frat } G$ is supersoluble, then G is supersoluble.*

Exercises 9.4

1. Let G be a finite soluble group which is not supersoluble but all whose proper quotients are supersoluble. Establish the following facts (without using 9.4.4).
   (a) The Fitting subgroup F is an elementary abelian p-group of order $> p$.
   (b) F is the unique minimal normal subgroup of G.

(c) $G = XF$ and $X \cap F = 1$ where the supersoluble subgroup X acts faithfully on F.
(d) Frat $G = 1$.

2. Deduce Huppert's Theorem (9.4.4) from Exercise 9.4.1.

3. Let G be a finite soluble group. Assume that every quotient group G with p-length at most 2 is supersoluble for all primes p. Prove that G is supersoluble.

4. Let G be a finite group. Prove that G is supersoluble if and only if for every proper subgroup H there is a chain of subgroups $H = H_0 < H_1 < \cdots < H_l = G$ with each index $|H_{i+1} : H_i|$ a prime.

9.5. Formations

A class of finite groups $\mathfrak{F}$ is said to be a *formation*† if every image of an $\mathfrak{F}$-group is an $\mathfrak{F}$-group and if $G/N_1 \cap N_2$ belongs to $\mathfrak{F}$ whenever G/N_1 and G/N_2 belong to $\mathfrak{F}$. A comparison of this definition with the characterization of varieties in 2.3.5 might suggest that a formation be thought of as a kind of finite analogue of a variety. (However formations are not in general closed will respect to forming subgroups.)

Examples of formations are readily found. The classes of finite groups, finite soluble groups, finite nilpotent groups, and finite supersoluble groups are all formations.

A formation $\mathfrak{F}$ is said to be *saturated* if a finite group $G \in \mathfrak{F}$ whenever $G/\text{Frat}\, G \in \mathfrak{F}$. Obviously the class of all finite groups is saturated. The nilpotency of Frat G implies that finite soluble groups from a saturated formation. The other two formations mentioned above are also saturated in view of 5.2.15 and 9.4.5.

Locally Defined Formations

We shall describe an important method of constructing saturated formations. For each prime p let $\mathfrak{F}_p$ be a formation or the empty set. Define $\mathfrak{F}$ to be the class of all groups G with following property: if H/K is a principal factor of G whose order is divisible by p, then $G/C_G(H/K)$ belongs to $\mathfrak{F}_p$.

It is clear that the class $\mathfrak{F}$ is closed with respect to forming images. If G/N_1 and G/N_2 belong to $\mathfrak{F}$ and $N_1 \cap N_2 = 1$, a principal factor of G is G-isomorphic with a principal factor of G/N_1 or of G/N_2. This is a consequence of the Jordan–Hölder Theorem. The validity of the centralizer property is now apparent. Thus $\mathfrak{F}$ is in fact a formation. $\mathfrak{F}$ is said to be *locally defined* by the $\mathfrak{F}_p$. For example, we see that the class of groups of order 1 is locally defined by taking every $\mathfrak{F}_p$ to be empty.

† Some authors allow formations to be empty.

9.5.1 (Gaschütz). *If $\mathfrak{F}$ is locally defined by formations $\mathfrak{F}_p$, then $\mathfrak{F}$ is a saturated formation.*

Proof. Let G be a group such that $G/\text{Frat } G \in \mathfrak{F}$: we have to show that $G \in \mathfrak{F}$. Let P denote the intersection of the centralizers of those principal factors of $G/\text{Frat } G$ whose orders are divisible by the prime p; then $G/P \in \mathfrak{F}_p$ by definition of $\mathfrak{F}$. Now $P/\text{Frat } G = \text{Fit}_p(G/\text{Frat } G) = \text{Fit}_p(G)/\text{Frat } G$ by 9.3.3 and 9.3.4. Thus $P = \text{Fit}_p(G)$ and 9.3.3 shows that P centralizes every principal factor of G whose order involves p. If H/K is such a principal factor, then $C_G(H/K) \geq P$ and therefore $G/C_G(H/K) \in \mathfrak{F}_p$. It now follows that $G \in \mathfrak{F}$. □

Remark. P. Schmid [a185] has proved that every saturated formation is locally defined. Thus all saturated formations can be constructed in the above manner.

EXAMPLES. Let $\mathfrak{F}$ be the formation locally defined by formations $\mathfrak{F}_p$ where p is prime.

(i) If each $\mathfrak{F}_p$ is the class of unit groups, then $\mathfrak{F}$ is the class of *finite nilpotent groups.*

(ii) If q is a fixed prime, define $\mathfrak{F}_q$ to be the class of all unit groups and if $p \neq q$, let $\mathfrak{F}_p$ be the class of all finite groups. Then $\mathfrak{F}$ is the class of finite groups in which every principal factor with order divisible by q is central. By 9.3.3 this is just the class of *finite q-nilpotent groups.*

9.5.2. *Let $\mathfrak{F}$ be a saturated formation and let N be a minimal normal subgroup of the finite soluble group G. Assume that $G/N \in \mathfrak{F}$ but $G \notin \mathfrak{F}$. Then N has a complement in G and all such complements are conjugate.*

Proof. If $N \leq \text{Frat } G$, then $G/\text{Frat } G \in \mathfrak{F}$, whence $G \in \mathfrak{F}$ because $\mathfrak{F}$ is saturated. This is incorrect, so there exists a maximal subgroup M not containing N. Then $G = MN$ and $M \cap N \lhd G$ since N is abelian. Hence $M \cap N = 1$.

For the second part, let K_1 and K_2 be two complements of N in G. Then K_1 and K_2 are maximal subgroups of G by 5.4.2. Write C for the core of K_1 in G. Then surely $C \cap N = 1$ and, since $G \notin \mathfrak{F}$, it follows that $G/C \notin \mathfrak{F}$. If $C \not\leq K_2$, then $G = CK_2$ and $G/C \simeq K_2/C \cap K_2 \in \mathfrak{F}$ because $K_2 \simeq G/N \in \mathfrak{F}$. By this contradiction $C \leq K_2$. Consequently K_1/C and K_2/C are complements of NC/C in G/C. Moreover $G/NC \in \mathfrak{F}$ and $G/C \notin \mathfrak{F}$, while $N \simeq^G NC/C$, so that NC/C is minimal normal in G/C. Now if C is nontrivial, we can apply induction on the group order to G/C, concluding that K_1/C and K_2/C—and hence K_1 and K_2—are conjugate. If $C = 1$, then $C_{K_1}(N) = 1$ and therefore $N = C_G(N)$. Now we may apply Exercise 9.1.14 to obtain the result. □

$\mathfrak{F}$-Covering Subgroups

If $\mathfrak{F}$ is a formation and G is a finite group, let

$$G_{\mathfrak{F}}$$

denote the intersection of all normal subgroups N such that $G/N \in \mathfrak{F}$. Then $G/G_{\mathfrak{F}} \in \mathfrak{F}$ and this is the largest $\mathfrak{F}$-quotient of G.

A subgroup H of G is called an *$\mathfrak{F}$-covering subgroup* if $H \in \mathfrak{F}$ and if $S = S_{\mathfrak{F}}H$ for all subgroups S that contain H: of course this equation asserts that H covers $S/S_{\mathfrak{F}}$ and hence every $\mathfrak{F}$-quotient of S. It will turn out that $\mathfrak{F}$-covering subgroups exist and are conjugate whenever G is soluble and $\mathfrak{F}$ is saturated. Before proving this we shall record two simple facts about $\mathfrak{F}$-covering subgroups.

9.5.3. *Let G be a finite group, $H \leq G$ and $N \lhd G$. Let $\mathfrak{F}$ be a formation.*

(i) *If H is an $\mathfrak{F}$-covering subgroup of G, then HN/N is an $\mathfrak{F}$-covering subgroup of G/N.*
(ii) *If H_1/N is an $\mathfrak{F}$-covering subgroup of G/N and H is an $\mathfrak{F}$-covering subgroup of H_1, then H is an $\mathfrak{F}$-covering subgroup of G.*

Proof. (i) Let $HN/N \leq S/N \leq G/N$ and put $R_1/N = (S/N)_{\mathfrak{F}}$ and $R = S_{\mathfrak{F}}$; then $RN/N \leq R_1/N$. Hence

$$(HN/N)(R_1/N) \geq (HR)N/N = S/N,$$

which implies that HN/N is an $\mathfrak{F}$-covering subgroup of G/N.

(ii) First of all observe that $H_1 = HN$ because $H_1/N \in \mathfrak{F}$ and $H \leq H_1$. Assume that $H \leq S \leq G$ and put $R = S_{\mathfrak{F}}$. Obviously H_1/N is an $\mathfrak{F}$-covering subgroup of SN/N and $SN/RN \in \mathfrak{F}$; therefore $SN = H_1RN = HRN$ and $S = S \cap (HRN) = (HR)(S \cap N)$. In addition $S \cap H_1 = S \cap (HN) = H(S \cap N)$, so $(S \cap H_1)R = S$. Consequently $S \cap H_1/R \cap H_1 \simeq S/R \in \mathfrak{F}$. Since H is an $\mathfrak{F}$-covering subgroup of $S \cap H_1$, it follows that $S \cap H_1 = H(R \cap H_1)$ and hence that $S = (S \cap H_1)R = HR$, as we wanted to show. □

We come now to the fundamental theorem on $\mathfrak{F}$-covering subgroups which yields numerous families of conjugate subgroups in a finite soluble group.

9.5.4 (Gaschütz). *Let $\mathfrak{F}$ be a formation.*

(i) *If every finite group has an $\mathfrak{F}$-covering subgroup, then $\mathfrak{F}$ is saturated.*
(ii) *If $\mathfrak{F}$ is saturated, every finite soluble group G possesses $\mathfrak{F}$-covering subgroups and any two of these are conjugate in G.*

Proof. (i) Let G be a finite group such that $G/\text{Frat } G \in \mathfrak{F}$. If H is an $\mathfrak{F}$-covering subgroup of G, then $G = H(\text{Frat } G)$, which implies that $G = H$ by the nongenerator property of Frat G. Thus $G \in \mathfrak{F}$ and $\mathfrak{F}$ is saturated.

(ii) This part will be established by induction on $|G|$. If $G \in \mathfrak{F}$, then G is evidently the only $\mathfrak{F}$-covering subgroup, so we shall exclude this case. Choose a minimal normal subgroup N of G. Then by induction G/N has an $\mathfrak{F}$-covering subgroup H_1/N.

Suppose first that $G/N \notin \mathfrak{F}$, so that $H_1 \neq G$. By induction H_1 has an $\mathfrak{F}$-covering subgroup H. We deduce directly from 9.5.3(ii) that H is an $\mathfrak{F}$-covering subgroup of G. Now let H_1 and H_2 be two $\mathfrak{F}$-covering subgroups of G. By 9.5.3(i) the subgroups H_1N/N and H_2N/N are $\mathfrak{F}$-covering subgroups of G/N, whence they are conjugate, say $H_1N = H_2^gN$ where $g \in G$. Now $H_1N \neq G$ because $G/N \notin \mathfrak{F}$. Hence H_1 and H_2^g, as $\mathfrak{F}$-covering subgroups of H_1N, are conjugate, which implies that H_1 and H_2 are conjugate.

Finally, assume that $G/N \in \mathfrak{F}$. Then 9.5.2 shows that there is a complement K of N in G. Moreover K must be maximal in G since N is minimal normal. Since $G/N \in \mathfrak{F}$, we have $G_{\mathfrak{F}} = N$ and $G = KG_{\mathfrak{F}}$. Therefore, since K is maximal in G, it is an $\mathfrak{F}$-covering subgroup of G. If H is another such subgroup, then $G = HN$, while $H \cap N = 1$ since N is abelian. Applying 9.5.2 we conclude that H and K are conjugate. □

There is a simple but useful application of 9.5.4.

9.5.5. *Let $\mathfrak{F}$ be a saturated formation and G a finite soluble group. If $N \lhd G$ then each $\mathfrak{F}$-covering subgroup of G/N has the form HN/N where H is an $\mathfrak{F}$-covering subgroup of G.*

Proof. Let K/N be an $\mathfrak{F}$-covering subgroup of G/N and let H_1 be one of G. Then H_1N/N is an $\mathfrak{F}$-covering subgroup of G/N, so H_1N/N is conjugate to K/N by 9.5.4. Hence $K = (H_1N)^g = H_1^gN$ for some g in G. Define H to be H_1^g. □

$\mathfrak{F}$-Projectors

Let $\mathfrak{F}$ be a formation. A subgroup H of a finite group G is called an $\mathfrak{F}$-*projector* if HN/N is maximal $\mathfrak{F}$-subgroup of G/N whenever $N \lhd G$.

There is a close connection between $\mathfrak{F}$-covering subgroups and $\mathfrak{F}$-projectors, as the next theorem indicates.

9.5.6 (Hawkes). *Let $\mathfrak{F}$ be a formation and let G be a finite soluble group.*

(i) *Every $\mathfrak{F}$-covering subgroup of G in an $\mathfrak{F}$-projector.*
(ii) *If $\mathfrak{F}$ is saturated, every $\mathfrak{F}$-projector of G is an $\mathfrak{F}$-covering subgroup.*

Before commencing the proof we must establish an auxiliary result.

9.5.7 (Carter–Hawkes). *Let $\mathfrak{F}$ be a saturated formation and G a finite soluble group. If H is an $\mathfrak{F}$-subgroup such that $G = H(\text{Fit } G)$, then H is contained in an $\mathfrak{F}$-covering subgroup of G.*

Proof. Let us argue by induction on $|G| > 1$. Obviously we may assume that $G \notin \mathfrak{F}$. Let N be a minimal normal subgroup of G. Then HN/N inherits the hypotheses on H, so by induction it is contained in some $\mathfrak{F}$-covering subgroup of G/N. The latter will by 9.5.5 be of the form KN/N where K is an $\mathfrak{F}$-covering subgroup of G. Consequently $H \leq KN$.

Suppose that $KN < G$. Then by induction hypothesis H is contained in some $\mathfrak{F}$-covering subgroup M of KN. But evidently K is an $\mathfrak{F}$-covering subgroup of KN and as such is conjugate to M. This shows M to be an $\mathfrak{F}$-covering subgroup of G.

We may therefore assume that $KN = G$. Let $F = \text{Fit}\, G$. Now $N \leq F$ since G is soluble, and indeed $N \leq \zeta F$ because $1 \neq N \cap \zeta F \lhd G$. Therefore $K \cap F \lhd KN = G$. If $K \cap F \neq 1$, we can apply the induction hypothesis to $G/K \cap F$, concluding that $H \leq T$ where $T/K \cap F$ is an $\mathfrak{F}$-covering subgroup of $G/K \cap F$. Thus $T_{\mathfrak{F}} \leq K$. Also T covers $G/(K \cap F)N \in \mathfrak{F}$, so $G = TN$ and $T/T \cap N \simeq K/K \cap N \in \mathfrak{F}$. Thus $T_{\mathfrak{F}} \leq K \cap N$. But $K \cap N = 1$ since the alternative is $N \leq K$, which leads to $G = K \in \mathfrak{F}$. Therefore $T_{\mathfrak{F}} = 1$ and $T \in \mathfrak{F}$. It is now clear that T is an $\mathfrak{F}$-covering subgroup of G.

Consequently we can assume that $K \cap F = 1$. Hence $F = (KN) \cap F = N$. Then $G = HN$ and H is maximal in G: for $H \neq G$ since $G \notin \mathfrak{F}$. Finally $G_{\mathfrak{F}} = N$ since $G/N \in \mathfrak{F}$. Hence $G = HG_{\mathfrak{F}}$ and H itself is an $\mathfrak{F}$-covering subgroup of G. □

***Proof of* 9.5.6.** (i) Let H be an $\mathfrak{F}$-covering subgroup of G and let $N \lhd G$. If $HN \leq K$ and $K/N \in \mathfrak{F}$, then H covers K/N and $K = HN$. Hence HN/N is a maximal $\mathfrak{F}$-subgroup of G/N and H is an $\mathfrak{F}$-projector.

(ii) We shall argue by induction on $|G| > 1$. Assume that H is an $\mathfrak{F}$-projector of G and let N be a minimal normal subgroup of G. Then one easily verifies that HN/N is an $\mathfrak{F}$-projector of G/N. By induction hypothesis HN/N is an $\mathfrak{F}$-covering subgroup of G/N.

By 9.5.5 we can write $M = HN = H^*N$ where H^* is an $\mathfrak{F}$-covering subgroup of G. Since N is abelian, it is contained in $\text{Fit}\, M$, and $M = H(\text{Fit}\, M) = H^*(\text{Fit}\, M)$. By 9.5.7 there is an $\mathfrak{F}$-covering subgroup $\bar{H}$ of M containing H. But H is a maximal $\mathfrak{F}$-subgroup of G by the projector property, so $H = \bar{H}$. But H^* is clearly an $\mathfrak{F}$-covering subgroup of M. It follows now from 9.5.4 that H and H^* are conjugate in M. Obviously this means that H is an $\mathfrak{F}$-covering subgroup of G. □

Carter Subgroups

The most important instance of the preceding theory is when $\mathfrak{F}$ is the class of finite nilpotent groups. Then $\mathfrak{F}$-covering subgroups and $\mathfrak{F}$-projectors coincide and form a single conjugacy class of self-normalizing nilpotent subgroups in any finite soluble group. The existence of these subgroups was first established by R.W. Carter in 1961.

A *Carter subgroup* of a group is defined to be a self-normalizing nilpotent subgroup.

9.5.8 (Carter). *Let G be a finite soluble group.*

(i) *The Carter subgroups of G are precisely the covering subgroups (or projectors) for the formation of finite nilpotent groups.*
(ii) *Carter subgroups are abnormal in G.*

Proof. (i) Let $\mathfrak{N}$ be the formation of finite nilpotent groups and let H be an $\mathfrak{N}$-covering subgroup of G. Suppose that $H < N_G(H)$. Then there is a subgroup K such that $H \lhd K$ and K/H has prime order. Now $K = HR$ where $R = K_{\mathfrak{N}}$. However $R \leq H$, so $K = H$, a contradiction which shows that $H = N_G(H)$. Since $H \in \mathfrak{N}$, it is a Carter subgroup.

Conversely, let H be a Carter subgroup of G and suppose that $H \leq S \leq G$. Write $R = S_{\mathfrak{N}}$ and assume that $HR < S$. Then there is a maximal subgroup M of S containing HR. Since $S/R \in \mathfrak{N}$, we have $M \lhd S$. Induction on the group order shows that H is an $\mathfrak{N}$-covering subgroup of M. If $x \in S$, then H^x is also an $\mathfrak{N}$-covering subgroup of M and it is conjugate to H in M by 9.5.4. It follows that $S \leq N_G(H)M = HM = M$, which is false, indicating that H is an $\mathfrak{N}$-covering subgroup of G.

(ii) Again let H be a Carter subgroup. If $H \leq K \leq G$, then in fact $K = N_G(K)$ by the argument of the first paragraph. That H is abnormal in G is now a consequence of 9.2.11. □

Since a Carter subgroup of G is abnormal, it has a subgroup which is minimal with respect to being subabnormal in G. Remembering that the minimal subabnormal subgroups are precisely the system normalizers (9.2.15), we derive the following result.

9.5.9. *In a finite soluble group every Carter subgroup contains a system normalizer.*

In general the system normalizers are properly contained in the Carter subgroups (Exercise 9.5.8). However in the case of finite soluble groups of small nilpotent length quite a different situation prevails.

9.5.10 (Carter). *Let G be a finite soluble group of nilpotent length at most 2. Then the system normalizers coincide with the Carter subgroups of G.*

Proof. By hypothesis there exists a normal nilpotent subgroup M such that G/M is nilpotent. If N is a system normalizer of G, then N covers every central principal factor by 9.2.6 and we have $G = NM$. Denote by $p_1, \ldots, p_k$ the distinct prime divisors of $|G|$. Let N_i and M_i be the unique Sylow p_i'-subgroups of the nilpotent groups N and M respectively. Then $Q_i = M_iN_i$

is a Hall p_i'-subgroup of G since $G = NM$. Thus $\{Q_1, \dots, Q_k\}$ is a Sylow system of G. Now $M_i \lhd G$; hence N normalizes Q_i and $N \leq N_G(Q_i)$ for all i. Since all system normalizers have the same order, being conjugate, it follows that $N = \bigcap_{i=1}^k N_G(Q_i)$. If g normalizes N, it also normalizes N_i and hence Q_i. Thus $g \in N$ and N is self-normalizing, which means that N is a Carter subgroup. Since system normalizers and Carter subgroups are conjugate, the theorem follows. □

Fitting Classes and $\mathfrak{F}$-Injectors

A natural dualization of the theory of formations was given by Fischer, Gaschütz, and Hartley ([a47]) in 1967. A class of finite groups $\mathfrak{F}$ is called a *Fitting class* if it is closed with respect to forming normal subgroups and normal products of its members. For example, finite soluble groups and finite nilpotent groups form Fitting classes while finite supersoluble groups do not (see Exercise 5.4.6).

A subgroup H of a finite group G is called an *$\mathfrak{F}$-injector* if $H \cap S$ is a maximal $\mathfrak{F}$-subgroup of S whenever S is a subnormal subgroup of G. Thus an $\mathfrak{F}$-injector is the natural dual of an $\mathfrak{F}$-projector.

The analogue of 9.5.4 asserts that if $\mathfrak{F}$ is any Fitting class, every finite soluble group contains a unique conjugacy class of $\mathfrak{F}$-injectors. (No extra hypothesis on $\mathfrak{F}$ corresponding to saturation is required.) When $\mathfrak{F}$ is the class of finite nilpotent groups, it turns out that the $\mathfrak{F}$-injectors are precisely the maximal nilpotent subgroups which contain the Fitting subgroup. These usually differ from the $\mathfrak{F}$-projectors, that is, from the Carter subgroups.

Exercises 9.5

1. Give an example of a formation of finite soluble groups that is not subgroup closed. [*Hint*: Let $\mathfrak{F}$ be the class of finite soluble groups G such that no G-principal factor in G' is central in G.]
2. If $\mathfrak{F}$ is a formation and H is an $\mathfrak{F}$-covering subgroup of a finite group G, then H is a maximal $\mathfrak{F}$-subgroup.
3. Let $\mathfrak{F}$ be a formation containing all groups of prime order. If H is a subgroup which contains an $\mathfrak{F}$-covering subgroup of a finite group G, then $G = N_G(H)$. Deduce that if G is soluble, then $\mathfrak{F}$-covering subgroups are abnormal in G.
4. Show that every formation which is locally defined by formations $\mathfrak{F}_p$ satisfies the hypothesis of Exercise 9.5.3.
5. Prove that a finite soluble group has a set of conjugate abnormal supersoluble subgroups. Need all abnormal supersoluble subgroups be conjugate?
6. Identify the Carter subgroups of groups S_3, A_4, and S_4.
7. Prove that S_5 has Carter subgroups all of which are conjugate, but that A_5 has no Carter subgroups.

8. Give an example of a finite soluble group in which the Carter subgroups are not system normalizers.
9. Let G be a finite soluble group with abelian Sylow subgroups. Prove that each Carter subgroup contains exactly one system normalizer.
10. If G is a finite soluble group of nilpotent length ≤ 2, prove that every subabnormal subgroup is abnormal.
11. A group is called *imperfect* if it has no nontrivial perfect quotient groups. Prove that finite imperfect groups form a saturated formation.

CHAPTER 10

The Transfer and Its Applications

The subject of this chapter is one of the basic techniques of finite group theory, the transfer homomorphism. Since the kernel of this homomorphism has abelian quotient group, it is especially useful in the study of insoluble groups. It will be seen that this technique underlies many deep and important theorems about finite groups.

10.1. The Transfer Homomorphism

Let G be a group, possibly infinite, and let H be a subgroup with finite index n in G. Choosing a right transversal $\{t_1, \dots, t_n\}$ to H in G, we have $Ht_ig = Ht_{(i)g}$ with $g \in G$, where the mapping $i \mapsto (i)g$ is a permutation of the set $\{1, 2, \dots, n\}$. Thus $t_igt_{(i)g}^{-1} \in H$ for all g in G.

Suppose that θ: $H \to A$ is a given homomorphism from H to some abelian group A. Then the *transfer* of θ is the mapping

$$\theta^*: G \to A$$

defined by the rule

$$x^{\theta^*} = \prod_{i=1}^{n} (t_ixt_{(i)x}^{-1})^{\theta}.$$

Since A is abelian, the order of the factors in the product is irrelevant.

10.1.1. *The mapping θ^*: $G \to A$ is a homomorphism which does not depend on the choice of transversal.*

Proof. Let us first establish independence of the transversal. Let $\{t_1', \dots, t_n'\}$ be another right transversal to H in G and suppose that $Ht_i = Ht_i'$ and

$t_i' = h_i t_i$ with h_i in H. Then, if $x \in G$,

$$t_i' x t_{(i)x}'^{-1} = h_i(t_i x t_{(i)x}^{-1}) h_{(i)x}^{-1},$$

and therefore, since A is commutative,

$$\prod_{i=1}^{n} (t_i' x t_{(i)x}'^{-1})^\theta = \prod_{i=1}^{n} (t_i x t_{(i)x}^{-1})^\theta \cdot \prod_{i=1}^{n} h_i^\theta h_{(i)x}^{-\theta}. \tag{1}$$

Now as i runs over the set $\{1, 2, \ldots, n\}$, so does $(i)x$, from which it follows that the second factor in (1) is trivial. Hence the uniqueness of θ^* is established.

Next, if x and y are elements of G, we calculate that

$$\begin{aligned}(xy)^{\theta^*} &= \prod_{i=1}^{n} (t_i x y t_{(i)xy}^{-1})^\theta \\ &= \prod_{i=1}^{n} (t_i x t_{(i)x}^{-1})^\theta (t_{(i)x} y t_{(i)xy}^{-1})^\theta \\ &= \prod_{i=1}^{n} (t_i x t_{(i)x}^{-1})^\theta \cdot \prod_{j=1}^{n} (t_j y t_{(j)y}^{-1})^\theta \\ &= x^{\theta^*} y^{\theta^*},\end{aligned}$$

and θ^* is a homomorphism as claimed. □

Computing θ^*

We continue the notation used above. The value of θ^* at x can often be effectively computed by making an appropriate choice of transversal; this choice will not affect θ^* by 10.1.1.

Consider the permutation of the set of right cosets $\{Ht_1, \ldots, Ht_n\}$ produced by right multiplication by $x \in G$. A typical $\langle x \rangle$-orbit will have the form

$$(Hs_i, Hs_i x, \ldots, Hs_i x^{l_i - 1}); \tag{2}$$

here x^{l_i} is the first positive power of x such that $Hs_i x^{l_i} = Hs_i$, and of course $\sum_{i=1}^{k} l_i = n$. The elements $s_i x^j$, $i = 1, \ldots, k$, $j = 1, \ldots, l_i - 1$ form a right transversal to H. Using this transversal we calculate x^{θ^*}. Since $Hs_i x^{l_i} = Hs_i$, the contribution of the orbit (2) to x^{θ^*} is

$$((s_i x)(s_i x)^{-1} \cdots (s_i x^{l_i - 1})(s_i x^{l_i - 1})^{-1} (s_i x^{l_i} s_i^{-1}))^\theta,$$

which reduces to $(s_i x^{l_i} s_i^{-1})^\theta$. Therefore

$$x^{\theta^*} = \prod_{i=1}^{k} (s_i x^{l_i} s_i^{-1})^\theta.$$

We shall give this important formula the status of a lemma.

10.1.2. *Let the x-orbits of the set of right cosets of H in G be*

$$(Hs_i, Hs_ix, \dots, Hs_ix^{l_i-1}),$$

$i = 1, \dots, k$. *If* $\theta: H \to A$ *is a homomorphism into an abelian group, then*

$$x^{\theta^*} = \prod_{i=1}^{k} (s_ix^{l_i}s_i^{-1})^{\theta}.$$

Transfer into a Subgroup

The most important case of the transfer arises when θ is the natural homomorphism from H to H_{ab}, that is, $x^\theta = H'x$. In this case $\theta^*: G \to H_{ab}$ is referred to as the *transfer of G into H.*

Two cases of special interest are when H is central in G and when H is a Sylow subgroup of G. We consider the central case first.

10.1.3 (Schur). *Let H be a subgroup of the center of a group G and suppose that* $|G:H| = n$ *is finite. Then the transfer* τ *of G into H is the mapping* $x \mapsto x^n$. *Hence this mapping is an endomorphism of G.*

Proof. Continuing the notation of 10.1.2, we note that $s_ix^{l_i}s_i^{-1} \in H$ since it is a product of elements of H. It follows that $x^{l_i} \in H$ and hence that $s_ix^{l_i}s_i^{-1} = x^{l_i}$. Finally $x^\tau = \prod_{i=1}^{k} x^{l_i} = x^n$. □

We pause to mention a corollary of 10.1.3 which will be important in the study of finiteness properties of a group that refer to conjugates (Chapter 14).

10.1.4 (Schur). *If G is a group whose center has finite index n, then G' is finite and* $(G')^n = 1$.

Proof. Let $C = \zeta G$ and write $G/C = \{Cg_1, \dots, Cg_n\}$. For any c_i in C we have, on account of the fundamental commutator identities, the equality $[c_ig_i, c_jg_j] = [g_i, g_j]$, which implies that G' is generated by the $\binom{n}{2}$ elements $[g_i, g_j]$, $i < j$. Since $G'/G' \cap C \simeq G'C/C$, which is finite, we deduce from 1.6.11 that $G' \cap C$ is a finitely generated abelian group. From 10.1.3 we know that the mapping $x \mapsto x^n$ is a homomorphism from G to C, and since C is abelian, G' must be contained in the kernel; therefore $(G')^n = 1$. That $G' \cap C$, and hence G', is finite is now a consequence of 4.2.9. □

Transfer into a Sylow p-Subgroup

If P is a Sylow p-subgroup of a finite group G and $\tau: G \to P_{ab}$ is the transfer, then $G/\text{Ker}\,\tau$ is an abelian p-group. With this in mind we define

$$G'(p)$$

to be the intersection of all normal subgroups N such that G/N is an abelian p-group. Thus $G/G'(p)$ is the largest abelian p-quotient of G.

10.1.5. *Let $\tau: G \to P_{ab}$ be the transfer of a finite group G into a Sylow p-subgroup P. Then $G'(p)$ is the kernel of τ and $P \cap G'$ is the kernel of the restriction of τ to P.*

Proof. Write K for $\operatorname{Ker} \tau$. In the first place $G'(p) \leq K$ because G/K is an abelian p-group.

Decompose the set of right cosets of P into x-orbits as in 10.1.2; then in the notation of that result

$$x^\tau = P' \prod_{i=1}^{k} s_i x^{l_i} s_i^{-1}.$$

Now $G = PG'(p)$, so we may choose the s_i to lie in $G'(p)$. On the basis of this equation we may write $x^\tau = P'x^n c$ where $n = |G:P|$ and $c \in G'(p)$. Thus $x \in K$ implies that $x^n \in P'G'(p) = G'(p)$. It follows that $K/G'(p)$ is a p'-group, a conclusion which can only mean that $K = G'(p)$.

Finally $P \cap \operatorname{Ker} \tau = P \cap G'(p) = P \cap G'$ since $G'(p)/G'$ is a p'-group. □

It follows from 10.1.5 that $\operatorname{Im} \tau \simeq G/G'(p)$: obviously the latter is isomorphic with the Sylow p-subgroup of G_{ab}, that is, with PG'/G'. Hence

$$\operatorname{Im} \tau \simeq P/P \cap G'. \tag{3}$$

Groups with an Abelian Sylow p-Subgroup

These ideas may be applied with particular advantage in the presence of an abelian Sylow p-subgroup.

10.1.6. *Let the finite group G have an abelian Sylow p-subgroup P and let N denote $N_G(P)$. Then $P = C_P(N) \times [P, N]$. Moreover, if $\tau: G \to P$ is the transfer, $\operatorname{Im} \tau = C_P(N)$ and $P \cap \operatorname{Ker} \tau = [P, N]$.*

Proof. As in 10.1.2 we can write $x^\tau = \prod_{i=1}^{k} s_i x^{l_i} s_i^{-1}$. Let $x \in P$ and write y for x^{l_i}. Then y and $y^{s_i^{-1}}$ both belong to P. Since P is abelian, the subgroup $C = C_G(y^{s_i^{-1}})$ contains $\langle P, P^{s_i^{-1}} \rangle$, and by Sylow's Theorem P and $P^{s_i^{-1}}$ are conjugate in C, say, $P^{s_i^{-1}} = P^c$ where $c \in C$. Thus $r_i = s_i^{-1}c^{-1} \in N$. Since $y^{s_i^{-1}} = y^{r_i}$, we compute that

$$x^\tau = \prod_{i=1}^{k} (x^{l_i})^{r_i} = x^n d, \tag{4}$$

where $n = |G:P|$ and $d = \prod_{i=1}^{k} [x^{l_i}, r_i] \in [P, N]$. It follows successively that $x^n \in P^\tau[P, N]$ and $P = P^\tau[P, N]$ because $(n, p) = 1$. Suppose next that

$x^\tau \in \text{Ker}\,\tau$ where $x \in P$; then $1 = (x^\tau)^\tau = (x^\tau)^n$ because $(G')^\tau = 1$. Consequently $x^\tau = 1$ and $P^\tau \cap \text{Ker}\,\tau = 1$. Since $G = PG'(p)$, and thus $\text{Im}\,\tau = P^\tau$, we have $P = (\text{Im}\,\tau) \times [P, N]$.

Next we claim that $\text{Im}\,\tau \lhd N$. For if $x \in P$ and $y \in N$, then

$$(x^\tau)^y = \prod_{i=1}^{n} (t_i x t_{(i)x}^{-1})^y = \prod_{i=1}^{n} t_i^y x^y (t_{(i)x}^y)^{-1},$$

where $\{t_1, \dots, t_n\}$ is any right transversal to P. But $\{t_1^y, \dots, t_n^y\}$ is also a right transversal because $y \in N_G(P)$. Thus $(x^\tau)^y = (x^y)^\tau$—see also Exercise 10.1.14. Hence $\text{Im}\,\tau \lhd N$.

We deduce that $[\text{Im}\,\tau, N] \leq \text{Im}\,\tau \cap [P, N] = 1$ and $\text{Im}\,\tau \leq C_P(N)$. On the other hand, if $x \in C_P(N)$, then (4) shows that $x^\tau = x^n$, which yields $x \in \text{Im}\,\tau$ and $C_P(N) \leq \text{Im}\,\tau$. Hence $C_P(N) = \text{Im}\,\tau$. Finally $[P, N] \leq P \cap \text{Ker}\,\tau$, and also $|P : P \cap \text{Ker}\,\tau| = |P^\tau| = |P : [P, N]|$ since $P = P^\tau \times [P, N]$. Therefore $P \cap \text{Ker}\,\tau = [P, N]$. □

10.1.7 (Taunt). *Let G be a finite group all of whose Sylow subgroups are abelian. Then $G' \cap \zeta G = 1$ and ζG is the hypercenter of G.*

Proof. Let p be a prime and P a Sylow p-subgroup of G. Then

$$(G' \cap \zeta G) \cap P \leq C_P(N_G(P)) \cap (P \cap G') = 1$$

by 10.1.5 and 10.1.6. Since this is true for every prime, it follows that $G' \cap \zeta G = 1$. Finally $[\zeta_2 G, G] \leq G' \cap \zeta G = 1$ and therefore $\zeta G = \zeta_2 G$. □

The following useful result is an easy consequence of 10.1.6.

10.1.8 (Burnside). *If for some prime p a Sylow p-subgroup P of a finite group G lies in the center of its normalizer, then G is p-nilpotent.*

Proof. By hypothesis P is abelian and $P = C_P(N_G(P))$. We deduce at once from 10.1.6 that $P \cap \text{Ker}\,\tau = 1$ where of course $\tau: G \to P$ is the transfer. This means that $\text{Ker}\,\tau$ is a p'-group, which in turn implies that G is p-nilpotent since $G/\text{Ker}\,\tau \simeq \text{Im}\,\tau$, a p-group. □

While much more powerful criteria for p-nilpotence are available, as the following sections will show, 10.1.8 provides significant information about the orders of finite simple groups.

10.1.9. *Let p be the smallest prime dividing the order of the finite group G. Assume that G is not p-nilpotent. Then the Sylow p-subgroups of G are not cyclic. Moreover $|G|$ is divisible by p^3 or by 12.*

Proof. Let P be a Sylow p-subgroup of G and write N and C for the normalizer and centralizer of P respectively. Then $C \neq N$ by 10.1.8. Now N/C is isomorphic with subgroup of $\text{Aut}\,P$, by 1.6.13. If P is cyclic, then $P \leq C$

and N/C has order dividing $p-1$ by 1.5.5. However p is the smallest prime divisor of $|G|$, so we are forced to the contradiction $N = C$. Hence P is not cyclic.

Next suppose that p^3 does not divide $|G|$. Then P must be an elementary abelian p-group of order p^2 by 1.6.15 and the noncyclicity of P. Hence $\text{Aut } P \simeq \text{GL}(2, p)$, which has order $(p^2-1)(p^2-p)$. Since $C \geq P$, it follows that $|N:C|$ divides $(p-1)^2(p+1)$, which, if p were odd, would yield a smaller prime divisor of $|G|$ than p. Hence $p = 2$ and $|N:C| = 3$, so that $|G|$ is divisible by 12. □

If G is a finite simple group of composite order, then 10.1.9 tells us that $|G|$ is divisible by 12 or the cube of the smallest prime dividing the order of G. However by the Feit–Thompson Theorem this smallest prime is actually 2. So in fact the order of G is divisible by either 8 or 12. In addition the Sylow 2-subgroups of G cannot be cyclic. For a more precise result see Exercise 10.3.1.

Finite Groups with Cyclic Sylow Subgroups

We have developed sufficient machinery to classify all finite groups having cyclic Sylow subgroups. The definitive result is

10.1.10 (Hölder, Burnside, Zassenhaus). *If G is a finite group all of whose Sylow subgroups are cyclic, then G has a presentation*

$$G = \langle a, b \mid a^m = 1 = b^n, b^{-1}ab = a^r \rangle$$

where $r^n \equiv 1 \pmod{m}$, m is odd, $0 \leq r < m$, and m and $n(r-1)$ are coprime.

Conversely in a group with such a presentation all Sylow subgroups are cyclic.

This means that a finite group whose Sylow subgroups are cyclic is an extension of one cyclic group by another; such groups are called *metacyclic*. In particular the group is supersoluble.

***Proof of* 10.1.10.** (i) Assume that all the Sylow subgroups of G are cyclic. If G is abelian, then, being the direct product of its Sylow subgroups, G is cyclic and has a presentation of the required sort with $m = 1$. Thus we may assume that G is not abelian.

Let p denote the smallest prime divisor of $|G|$. Then, according to 10.1.9, the group G is p-nilpotent and $G/O_{p'}(G)$ is a p-group. By induction on the group order G is soluble; let d be the derived length. Then $G^{(d-1)}$ is abelian and therefore cyclic, from which it follows that $\text{Aut}(G^{(d-1)})$ is abelian. However this means that G' centralizes $G^{(d-1)}$, which, if $d > 2$, gives the contradiction $G^{(d-1)} \leq (G')' \cap \zeta(G') = 1$ by 10.1.7. So it has been proved that $d = 2$ and G is metabelian. Hence G/G' and G' are cyclic groups.

If Q is a Sylow q-subgroup of G, then 10.1.6 implies that either $Q \leq G'$ or $Q \cap G' = 1$: for Q, being cyclic, does not admit a nontrivial direct decomposition. Hence q cannot divide both $m = |G'|$ and $n = |G : G'|$; consequently these integers are coprime.

Let $G' = \langle a \rangle$ and $G/G' = \langle b_1 G' \rangle$. The order of b_1 must be expressible in the form $m_1 n$ where m_1 divides m. Now $b = b_1^{m_1}$ has order n and bG' generates G/G' because $(m_1, n) = 1$. Therefore $G = \langle a, b \rangle$. Also $a^b = a^r$ where the integer r satisfies $r^n \equiv 1 \bmod m$ and $1 < r < m$. Suppose that there is a prime q dividing m and $r - 1$. Then $r \equiv 1 \bmod q$ and if $a_1 = a^{m/q}$, we should have $|a_1| = q$ and $a_1^b = a_1^r = a_1$, whence $a_1 \in G' \cap \zeta G = 1$ by 10.1.7; but this would mean that $|a| = m/q$, a contradiction which shows that $(m, r - 1) = 1$. Since $(m, r) = 1$, it follows that m is odd.

(ii) Conversely assume that G has the given presentation and that P is a Sylow p-subgroup. Then $\langle a \rangle \lhd G$ and G is finite of order mn, while either $P \leq \langle a \rangle$ or $P \cap \langle a \rangle = 1$ since $(m, n) = 1$. In either case P is cyclic. □

Prominent among the groups with cyclic Sylow subgroups are *the groups with square-free order*: such groups are therefore classified by 10.1.10.

Exercises 10.1

1. Let $H \leq K \leq G$ where G is finite. Denote the transfer of G into K by $\tau_{G,K}$. Prove that $\tau_{G,K}\tau_{K,H} = \tau_{G,H}$ (with a slight abuse of notation).

2. If G is a group whose center has finite index n, prove that $|G'|$ divides $n^{n[\log_2 n]-n+2}$. [*Hint*: Use Exercise 1.3.4.]

*3. If $G/\zeta G$ locally finite π-group (that is, finitely generated subgroups are finite π-groups), prove that G' is a locally finite π-group.

4. If G is a simple group of order p^2qr where p, q, r are primes, prove that $G \simeq A_5$. [*Hint*: $|G|$ is divisible by 12.]

5. There are no perfect groups of order 180, (so a nonsimple perfect group of order ≤ 200 has order 1 or 120—see Exercise 5.4.4).

6. Let H be a p'-group of automorphisms of a finite abelian p-group A. Prove that $A = [A, H] \times C_A(H)$. If H acts trivially on $A[p]$, prove that $H = 1$.

7. Let N be a system normalizer of a finite soluble group G which has abelian Sylow subgroups. Prove that $G = NG'$ and $N \cap G' = 1$.

8. (Taunt). Let G be a finite soluble group with abelian Sylow subgroups. If $L \lhd G$ and L is abelian, prove that $L = (L \cap G') \times (L \cap \zeta G)$. Deduce that $L = (L \cap \zeta G) \times (L \cap \zeta G') \times \cdots \times (L \cap \zeta G^{(d-1)})$ where d is the derived length of G. [*Hint*: Let N be a system normalizer. Apply Exercise 10.1.7 and show that $L \cap N = L \cap \zeta G$.]

9. Let $G(m, n, r)$ be a finite group with cyclic Sylow subgroups in the notation of 10.1.10. Prove that $G(m, n, t) \simeq G(\bar{m}, \bar{n}, \bar{r})$ if and only if $m = \bar{m}$, $n = \bar{n}$ and $\langle r + m\mathbb{Z} \rangle = \langle \bar{r} + m\mathbb{Z} \rangle$ in $\mathbb{Z}_m^*$.

10. How many nonisomorphic groups are there of order 210?
11. Let G be a finite group with cyclic Sylow subgroups. Prove that every subnormal subgroup of G is normal.
12. (Burnside). Let n be a positive integer. Prove that every group of order n is cyclic if and only if $(n, \varphi(n)) = 1$ where φ is the Eulerian function.
13. What conditions on the integer n will ensure that all groups of order n are abelian?
14. Let H be a subgroup of finite index in a group G. If τ is the transfer of G into H and $y \in N_G(H)$, prove that $(x^\tau)^y = (x^y)^\tau$ for all x in G.
15. Let G be a group, H a subgroup with finite index in G, and A any abelian group. Then restriction to H yields a homomorphism Res: $\mathrm{Hom}(G, A) \to \mathrm{Hom}(H, A)$. The *corestriction map* Cor: $\mathrm{Hom}(H, A) \to \mathrm{Hom}(G, A)$ is defined by $\theta \mapsto \theta^*$ where θ^* is the transfer of θ. Prove that Cor is a homomorphism and that Res $\circ$ Cor is multiplication by $|G : H|$ in $\mathrm{Hom}(G, A)$.

10.2. Grün's Theorems

Two important and powerful transfer theorems due to O. Grün will be proved in this section. These theorems provide us with more useful expressions for the kernel and image of the transfer into a Sylow subgroup.

10.2.1 (Grün's First Theorem). *Let G be a finite group and let P be a Sylow p-subgroup of G. If $N = N_G(P)$ and $\tau: G \to P_{ab}$ is the transfer, then*

$$P \cap \mathrm{Ker}\, \tau = P \cap G' = \langle P \cap N', P \cap (P')^g \mid g \in G \rangle.$$

Proof. In the first place $P \cap \mathrm{Ker}\, \tau = P \cap G'$ by 10.1.5. Define D to be the subgroup generated by $P \cap N'$ and all $P \cap (P')^g$ with $g \in G$. Then certainly $D \leq P \cap G'$ and $D \lhd P$. What we must prove is that $P \cap G' \leq D$. Assuming this to be false, let us choose an element u of least order in $(P \cap G') \backslash D$.

We shall calculate u^τ by a refinement of the method of 10.1.2. First of all decompose G into (P, P)-double cosets Px_jP, $j = 1, 2, \ldots, s$. Now a double coset PxP is a union of cosets of the form Pxy, $y \in P$, and the latter are permuted transitively by right multiplication by elements of P. Hence the number of cosets of the form Pxy, $y \in P$, with Px fixed, divides $|P|$ and equals a power of p, say p^t. Under right multiplication by u the cosets Pxy fall into orbits of the form

$$(Pxy_i, Pxy_iu, \ldots, Pxy_iu^{p^{m_i}-1}), \qquad i = 2, \ldots, r, \tag{5}$$

where $y_i \in P$ and $u^{p^{m_i}}$ is the smallest positive power of u such that $Pxy_iu^{p^{m_i}} = Pxy_i$. These orbits are to be labeled so that $m_1 \leq m_2 \leq \cdots \leq m_r$. Replacing x by xy_1, we can suppose $y_1 = 1$. The elements xy_iu^j, $i = 1$,

$2, \dots, r$, $j = 0, 1, \dots, p^{m_i} - 1$ form part of a right transversal to P which may be used to compute u^τ.

Let us calculate the contribution of the u-orbit (5) to u^τ. This is $P'v_i$ where

$$v_i = xy_i u^{p^{m_i}} y_i^{-1} x^{-1} = (u^{p^{m_i}}[u^{p^{m_i}}, y_i^{-1}])^{x^{-1}}, \tag{6}$$

an element of P. Taking $i = 1$ we deduce that $(u^{p^{m_1}})^{x^{-1}} \in P$ since $y_1 = 1$. Now $m_1 \le m_i$ by our ordering, so $(u^{p^{m_i}})^{x^{-1}} \in P$ for all i and it follows from (6) that $c = [u^{p^{m_i}}, y_i^{-1}]^{x^{-1}} \in P$. In addition $c \in (P')^{x^{-1}}$, which means that $c \in D$. Consequently $v_i \equiv (u^{p^{m_i}})^{x^{-1}} \bmod D$. The total contribution to u^τ of the double coset PxP is therefore $P'w(x)$ where

$$w(x) = \prod_{i=1}^{r} v_i \equiv (u^{p^t})^{x^{-1}} \mod D \tag{7}$$

since $\sum_{i=1}^r p^{m_i} = p^t$.

Now suppose that $t > 0$. Since $w(x) \in P$, we have $(u^{p^t})^{x^{-1}} \in P \cap \operatorname{Ker} \tau$ by (7), and by minimality of $|u|$ we obtain $(u^{p^t})^{x^{-1}} \in D$. For the same reason $u^{p^t} \in D$. Thus we certainly have $w(x) \equiv 1 \equiv u^{p^t} \bmod D$.

If, on the other hand, $t = 0$, then $PxP = Px$, which is equivalent to $x \in N$. Hence PxP contributes $P'xux^{-1} = P'u[u, x^{-1}]$ to u^τ: of course $[u, x^{-1}] \in P \cap N' \le D$. Again we have $w(x) \equiv u^{p^t} \bmod D$.

Thus $\prod_{j=1}^s w(x_j) \equiv u^l \bmod D$ where $l = \sum_{j=1}^s p^{t_j}$ and p^{t_j} is the number of cosets Px_jy in Px_jP. Then $l = |G : P|$, the total number of right cosets of P in G. Since $u \in P \cap G'$, we have $u^\tau = P' \le D$. Hence $u^l \in D$, which yields $u \in D$ since p does not divide l. □

The next result illustrates the usefulness of Grün's theorem.

10.2.2 (Wong). *Suppose that G is a finite group which has a Sylow 2-subgroup P with a presentation $\langle a, b \mid a^{2^n} = 1 = b^2, a^b = a^{1+2^{n-1}}\rangle$ where $n > 2$. Then G is 2-nilpotent and, in particular, G cannot be simple.*

Proof. Let N denote $N_G(P)$. The Schur–Zassenhaus Theorem implies that there is a subgroup Q such that $N = QP$ and $Q \cap P = 1$; of course Q has odd order. However $Q/C_Q(P)$ is isomorphic with a subgroup of Aut P and by Exercises 5.3.5 the latter is a 2-group. Thus we are forced to conclude that $Q = C_Q(P)$ and $N = Q \times P$.

Applying 10.2.1 we have

$$P \cap G' = \langle P \cap N', P \cap (P')^g \mid g \in G\rangle.$$

Now $P \cap N' = P \cap (Q' \times P') = \langle a^{2^{n-1}}\rangle$, a group of order 2, which allows us to conclude that $P \cap G'$ is generated by elements of order 2. Since all the elements of P with order 2 belong to $P_0 = \langle a^{2^{n-1}}, b\rangle$, it follows that $P \cap G' \le P_0$.

Let L/G' be the odd component of G_{ab} and set $S = \langle a^2, b\rangle L$, evidently a normal subgroup of G. Now $P \cap S = \langle a^2, b\rangle$ $(P \cap L)$ and $P \cap L = P \cap G' \leq P_0$, from which it follows that $P \cap S = \langle a^2, b\rangle = P_1$, say. P_1 is a Sylow 2-subgroup of S since $S \lhd G$.

From the presentation one sees that P_1 is abelian: indeed it is the direct product of a cyclic group of order $2^{n-1} > 2$ and a group of order 2. Consequently Aut P_1 is a 2-group by Exercise 1.5.13. The argument of the first paragraph now shows that P_1 is a direct factor of $N_S(P_1)$ and we deduce from 10.1.8 that S is 2-nilpotent. Since $|G:S| \leq 2$, the same holds for G. □

There has been much work on the classification of finite simple groups of composite order according to the nature of their Sylow 2-subgroups. It was remarked above that the Sylow 2-subgroups of such a group cannot be cyclic; of course 10.2.2 excludes a further set of 2-groups.

For example, we mention that Brauer and Suzuki have shown that a (generalized) quaternion group Q_{2^n} cannot be the Sylow 2-subgroup of a finite simple group. In another investigation Gorenstein and Walter have proved that PSL(2, p^m), $p \neq 2$, and A_7 are the only finite simple groups to have a dihedral Sylow 2-subgroup. The proofs of these results are difficult and cannot be discussed here. For more information on these questions consult [b26].

Weak Closure and p-Normality

If H and K are subgroups of a group, then H is said to be *weakly closed* in K if $H \leq K$ and if $H^g \leq K$ always implies that $H = H^g$. Otherwise stated H is weakly closed in K if K contains H but no other conjugate of H.

If P is a Sylow p-subgroup of G and if the center of P is weakly closed in P, then G is said to be *p-normal.* Among p-normal groups are groups with abelian Sylow p-subgroups and groups in which distinct Sylow p-subgroups have trivial intersection.

10.2.3 (Grün's Second Theorem). *Let the finite group G be p-normal and let P be a Sylow p-subgroup of G. If $L = N_G(\zeta P)$, then $P \cap G' = P \cap L'$ and $G/G'(p) \simeq L/L'(p)$.*

Proof. In the first place $G/G'(p) \simeq P/P \cap G'$ by 10.1.5 and (3). In addition, since $P \leq L$, the subgroup P is a Sylow p-subgroup of L and $L/L'(p) \simeq P/P \cap L'$. The theorem will therefore follow should we succeed in proving that $P \cap G' = P \cap L'$. What is more, by Grün's First Theorem it suffices to show that $P \cap N' \leq P \cap L'$ and $P \cap (P')^g \leq P \cap L'$ for all g in G, where $N = N_G(P)$. Since ζP is characteristic in P, it is certainly true that $N \leq L$ and $P \cap N' \leq P \cap L'$. Thus we can concentrate on $I = P \cap (P')^g$.

Let $P_0 = \zeta P$ and $M = N_G(I)$. Then $P_0 \leq M$ and $P_0^g \leq M$ since $P_0^g = \zeta(P^g)$. Let P_1 and P_2 be Sylow p-subgroups of M containing P_0 and P_0^g respectively. Then of course $P_1 = P_2^h$ for some h in M. Now $P_1 \leq P^x$ for some x in G and $P_0 \leq P_1 \leq P^x$, so that P_0 and $P_0^{x^{-1}}$ are both contained in P. By p-normality $P_0 = P_0^{x^{-1}}$. In addition $P_0^{gh} \leq P_2^h = P_1 \leq P^x$, so that $P_0^{gh} = P_0^x = P_0$ by p-normality again. Thus $gh \in L$. It now follows that $I = I^h = P^h \cap (P')^{gh} \leq L'$ since $P \leq L$. Finally $I \leq P \cap L'$ as required. □

EXERCISES 10.2

1. Show that 10.2.2 does not hold if $n = 2$.
2. Let P be a finite 2-group such that Aut P is a 2-group and P cannot be generated by elements of order dividing $|P'|$. Prove that there is no finite simple group whose Sylow 2-subgroups are isomorphic with P. Give some examples. [*Hint*: Apply Grün's First Theorem.]
3. Prove that a p-nilpotent group is p-normal.
4. Let G be a finite p-normal group. If P is a Sylow p-subgroup and $L = N_G(\zeta P)$, prove that $L \cap G'(p) = L'(p)$.

10.3. Frobenius's Criterion for p-Nilpotence

Here we derive a useful criterion for p-nilpotence, describing in the sequel some of its many applications. The following technical lemma is used in the proof.

10.3.1 (Burnside). *Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Suppose that H is a subgroup of $P_1 \cap P_2$ which is normal in P_1 but not in P_2. Then there exists a p-subgroup M, a prime $q \neq p$ and a q-element g such that $H \leq M$ and $g \in N_G(M)\backslash C_G(M)$.*

Proof. Write $K = N_{P_2}(H)$ and assume that P_2 has been chosen so that K is maximal subject to $P_2 \nleq N_G(H)$. Since $K \leq N_G(H)$ and P_1 is a Sylow p-subgroup of $N_G(H)$, there is an x in $N_G(H)$ such that $K \leq P_1^x$ by Sylow's Theorem. Now $H \lhd P_1$ implies that $H \lhd P_1^x$, which indicates that we may replace P_1 by P_1^x without disturbing the hypotheses. Hence we can assume that $K \leq P_1$, so that $K \leq P_1 \cap P_2 \leq K$ and $K = P_1 \cap P_2$. Since $P_1 \neq P_2$, it follows that $K < P_1$ and $K < P_2$.

Apply the normalizer condition to P_i, $i = 1, 2$: then $K < N_i \leq P_i$ where $N_i = N_{P_i}(K)$. Hence $K \lhd L = \langle N_1, N_2 \rangle$. Notice that L cannot normalize H because, if it did, N_2 would be contained in $N_{P_2}(H) = K$.

Next N_1 is contained in a Sylow p-subgroup of L, which in turn is contained in some Sylow p-subgroup P_3 of G. Then $K < N_1 \leq N_{P_3}(H)$; this, in

view of the maximality of K, implies that P_3 normalizes H. It follows that there is a Sylow p-subgroup of L which normalizes H.

Combining the results of the last two paragraphs we conclude that there exist a prime $q \neq p$ and a Sylow q-subgroup Q of L such that Q does not normalize H. Let $g \in Q \backslash N_G(H)$ and put $M = H^{\langle g \rangle}$. Since $H \lhd K \lhd L$ and $Q \leq L$, we see that M is a p-group. Obviously $g \in N_G(M)$, but $g \notin C_G(M)$ since $g \notin C_G(H)$. □

10.3.2 (Frobenius). *A finite group G is p-nilpotent if and only if every p-subgroup is centralized by the p'-elements in its normalizer.*

Proof. Assume that G is p-nilpotent and that P is a p-subgroup. Then all the p'-elements belong to $O_{p'}(G)$, and we have $[O_{p'}(G) \cap N_G(P), P] \leq P \cap O_{p'}(G) = 1$, which establishes the necessity of our condition.

Conversely assume that the condition is satisfied in G and let P be a Sylow p-subgroup. The p-nilpotence of G will be established by induction on $|G|$; of course we may suppose that $|G| \neq 1$ and $|P| \neq 1$. Write $C = \zeta P$ and $L = N_G(C)$. Then $1 \neq C \lhd L$ and P/C is a Sylow p-subgroup of L/C. We verify easily that L/C inherits the condition imposed on G; therefore L/C has a normal Hall p'-subgroup Q/C. By the Schur–Zassenhaus Theorem there is a complement M of C in Q. But since M normalizes C and is a p'-group, it centralizes C; thus $Q = M \times C$. Evidently $|L : M|$ is a power of p, and in addition M is characteristic in Q and hence normal in L. From these properties there follows the equality $L = PM$. Consequently $P \cap L' \leq P \cap (P'M) = P'$ and $P \cap L' = P'$.

By 10.3.1 and the hypothesis a normal subgroup of a Sylow p-subgroup of G is normal in every Sylow p-subgroup that contains it. It follows that every Sylow subgroup containing C is itself contained in L. But $L = PM$ and both P and M centralize C, so that $C \leq \zeta L$. Combining this with the previous sentence we conclude that C lies in the centre of every Sylow p-subgroup which contains it, a property that is manifestly equivalent to weak closure of C in P, that is, to p-normality of G.

We are now in a position to apply Grün's Second Theorem, concluding that $P \cap G' = P \cap L'$. But we have seen that $P \cap L' = P'$, so in fact $P' = P \cap G'$, which is a Sylow p-subgroup of G' and hence of $G'(p)$. If $G'(p)$ were equal to G, it would follow that $P = P'$ and $P = 1$, contrary to assumption. Thus $G'(p)$ is a proper subgroup and by induction on $|G|$ it is p-nilpotent, which implies at once the p-nilpotence of G. □

Applications of Frobenius's Theorem

10.3.3 (Itô). *Let G be a finite group which is not p-nilpotent but whose maximal subgroups are p-nilpotent. Then G has a normal Sylow p-subgroup P such that $|G : P|$ is a power of a prime $q \neq p$. Moreover every maximal subgroup of G is nilpotent.*

Proof. Since G is not p-nilpotent, 10.3.2 shows that there exist a p-subgroup P, a prime $q \neq p$ and an element g of order q^m such that g normalizes but does not centralize P. Now $\langle g, P \rangle$ cannot be p-nilpotent, by 10.3.2 again. Consequently $G = \langle g, P \rangle$ and $P \lhd G$. Hence $|G : P| = |g| = q^m$ and P is a Sylow p-subgroup.

Let H be any maximal subgroup of G. Since H is p-nilpotent, $H/O_{p'}(H)$ is nilpotent. In addition $H/H \cap P$ is nilpotent while $P \cap O_{p'}(H) = 1$. It follows that H is nilpotent. □

Thus it emerges that a finite minimal non-p-nilpotent group is a minimal nonnilpotent group. Further structural properties can therefore be deduced from Exercise 9.1.11.

10.3.3 has, in turn, application to groups whose proper subgroups are supersoluble.

10.3.4 (Huppert). *If every maximal subgroup of a finite group G is supersoluble, then G is soluble.*

Proof. Assume that G is insoluble and let p be the smallest prime dividing $|G|$. If G is p-nilpotent, then $O_{p'}(G) \neq G$, so that $O_{p'}(G)$ is supersoluble. Since $G/O_{p'}(G)$ is a p-group, the solubility of G follows. Hence G is not p-nilpotent. On the other hand, a maximal subgroup of G is supersoluble and hence p-nilpotent by 5.4.8. However 10.3.3 shows that G must be soluble. □

A good deal of structural information about finite minimal nonsupersoluble groups is available: for details see [b6] (and also Exercise 10.3.10).

On the basis of 10.3.4 an interesting characterization of finite supersoluble groups pertaining to maximal chains may be established. Here by a *maximal chain* in a group G we mean a chain of subgroups $1 = M_0 < M_1 < \cdots < M_m = G$ such that M_i is maximal in M_{i+1} for each i.

10.3.5 (Iwasawa). *A finite group G is supersoluble if and only if all maximal chains in G have the same length.*

Proof. First let G be supersoluble. Since a maximal subgroup of a supersoluble group has prime index, the length of any maximal chain in G equals the number d of prime divisors of $|G|$, *including* multiplicities.

Conversely, assume that G has the chain property but is not supersoluble. Let G be chosen of least order among such groups. Since subgroups inherit the chain property, G is a minimal nonsupersoluble group, so by 10.3.4 it is soluble. Therefore a composition series of G is a maximal chain and the length of each maximal chain equals the composition length, which is just d, the number of prime divisors of $|G|$.

By 9.4.4 there exists a maximal subgroup M whose index is composite. On refinement of the chain $1 < M < G$ there results a maximal chain whose length is less than d, a contradiction. □

EXERCISES 10.3

1. If G is a finite simple group of even order, then $|G|$ is divisible by 12, 16, or 56.
2. If G is a finite simple group whose order is divisible by 16, prove that $|G|$ is divisible by 32, 48, 80, or 112.
3. A subgroup H is said to be *pronormal* in a group G if for all g in G the subgroups H and H^g are conjugate in $\langle H, H^g\rangle$. If H is pronormal and subnormal in G, show that $H \lhd G$.
4. Let G be a finite group and let p be the smallest prime dividing $|G|$. If every p-subgroup is pronormal in G, then G is p-nilpotent. [*Hint*: Use Frobenius's criterion and Exercise 10.3.3.]
5. (J.S. Rose). Let G be a finite group and p a prime. Prove that every p-subgroup is pronormal in G if and only if each p-subgroup is normal in the normalizer of any Sylow p-subgroup that contains it. [*Hint*: Use and prove the result: if $H \lhd P$ and $H^g \lhd P$ where P is a Sylow p-subgroup of the finite group G, then H and H^g are conjugate in $N_G(P)$.]
6. Show that Exercise 10.3.4 does not hold for arbitrary primes p.
7. Let P be a Sylow p-subgroup of a finite group G. If $N_G(H) = P$ whenever H is a nontrivial abelian subgroup of P, prove that G is p-nilpotent. [*Hint*: Prove that $P \cap P^g = 1$ if $g \in G \backslash P$.]
8. Let P be a Sylow p-subgroup of a finite group G. Prove that G is p-nilpotent if and only if $N_G(H)$ is p-nilpotent whenever $1 \neq H \leq P$.
9. If G is a finite group in which every minimal p-subgroup is contained in the centre of G, then G is p-nilpotent provided $p > 2$.
10. (K. Doerk). Let G be a finite minimal nonsupersoluble group. Prove that G is p-nilpotent for some p dividing $|G|$.

10.4. Thompson's Criterion for p-Nilpotence

The subject of this section is a very powerful condition for p-nilpotence due to Thompson which has important application to Frobenius groups. A major role is played by a rather curious subgroup that can be formed in any finite p-group P. We define

$$J(P)$$

to be the subgroup generated by all abelian subgroups of P with maximal rank. Obviously $J(P)$ is characteristic in P.

10.4.1 (Thompson). *Let G be a finite group, p an odd prime and P a Sylow p-subgroup of G. Then G is p-nilpotent if and only if $N_G(J(P))$ and $C_G(\zeta P)$ are p-nilpotent.*

Proof. (i) Of course it is only the sufficiency of the conditions that is in question. We assume henceforth that $N_G(J(P))$ and $C_G(\zeta P)$ are p-nilpotent but G itself is not p-nilpotent. Furthermore let G be a group of smallest order with these properties. Observe that any proper subgroup containing P inherits the conditions on G and is therefore p-nilpotent.

The proof is broken up into a series of reductions, each one of itself being fairly straightforward.

(ii) $O_{p'}(G) = 1$.

Suppose that on the contrary $T = O_{p'}(G) \neq 1$ and write $\bar{G} = G/T$ and $\bar{P} = PT/T$. Our immediate object is to show that the conditions on G apply to $\bar{G}$. Certainly $\bar{P}$ is a Sylow p-subgroup of $\bar{G}$ isomorphic with P via the natural homomorphism $x \mapsto xT$. From this we deduce that $J(\bar{P}) = J(P)T/T$. If $xT \in N_{\bar{G}}(J(\bar{P}))$, then $J(P)^x T = J(P)T$, from which it follows by Sylow's Theorem that $J(P)^x = J(P)^y$ for some y in T; thus $x \in N_G(J(P))T$. Consequently $N_{\bar{G}}(J(\bar{P}))$ is contained in $N_G(J(P))T/T$, which shows the former to be p-nilpotent.

Now we must examine $C_{\bar{G}}(\zeta\bar{P})$. Clearly $\zeta\bar{P} = (\zeta P)T/T$, so that if $xT \in C_{\bar{G}}(\zeta\bar{P})$, then $(\zeta P)^x T = (\zeta P)T$; just as in the previous paragraph, $x \in N_G(\zeta P)T$. Clearly we can assume that $x \in N_G(\zeta P)$. Then $[\zeta P, x] \leq T \cap \zeta P = 1$ and $x \in C_G(\zeta P)$. Consequently $C_{\bar{G}}(\zeta\bar{P}) = C_G(\zeta P)T/T$ is p-nilpotent.

Finally the minimality of G allows us to conclude that $\bar{G}$ is p-nilpotent, which implies at once that G is p-nilpotent.

(iii) We introduce the set $\mathscr{S}$ of all nontrivial p-subgroups whose normalizer in G is not p-nilpotent. $\mathscr{S}$ is not empty, otherwise the normalizer of every nontrivial p-subgroup would be p-nilpotent, which in view of the Frobenius criterion (10.3.2) would imply the p-nilpotence of G.

The set $\mathscr{S}$ is partially ordered by means of a relation $\preccurlyeq$ defined in the following manner. If $H_1, H_2 \in \mathscr{S}$, then $H_1 \preccurlyeq H_2$ means that either

(i) $|N_G(H_1)|_p < |N_G(H_2)|_p$

or

(ii) $|N_G(H_1)|_p = |N_G(H_2)|_p$ and $|H_1| < |H_2|$.

Here n_p denotes the largest power of p dividing n.

Choose an element H of $\mathscr{S}$ which is maximal with respect to this partial ordering and write

$$N = N_G(H).$$

If P_0 is a Sylow p-subgroup of N, then $H \leq P_0$ since $H \lhd N$. Replacing P if necessary by a suitable conjugate, we may suppose that $P_0 \leq P$ and thus $H \leq P$. Also $P_0 \leq P \cap N$, so that $P_0 = P \cap N$ since P_0 is a Sylow p-subgroup of N.

(iv) $H = O_p(G)$ *and* $\bar{G} = G/H$ *is p-nilpotent.*

We shall first establish the fact that N satisfies the conditions on G. Since $H \leq P$, we have $[\zeta P, H] = 1$ and $\zeta P \leq N$, which implies that $\zeta P \leq P_0 \cap C_G(P_0) = \zeta P_0$ because $P_0 = P \cap N$. In consequence $C_N(\zeta P_0) \leq C_G(\zeta P)$, which demonstrates that $C_N(\zeta P_0)$ is p-nilpotent.

Let us now examine $N_N(J(P_0))$. If P_0 were equal to P, this normalizer would certainly be p-nilpotent. Assuming that $P_0 < P$, we invoke the normalizer condition to produce a subgroup P_1 normalizing P such that $P_0 < P_1 \leq P$. Since $J(P_0)$ is characteristic in P_0, it is normal in P_1 and thus $P_1 \leq N_G(J(P_0))$, which shows that $|N_G(J(P_0))|_p > |P_0| = |N|_p$. By maximality of H in $\mathscr{S}$ the group $N_G(J(P_0))$ must be p-nilpotent, whence so is $N_N(J(P_0))$.

If $N \neq G$, then N is p-nilpotent by minimality of G. But this contradicts the fact that $H \in \mathscr{S}$. Hence $N = G$ and $H \lhd G$, which leads at once to $H \leq O_p(G)$. Suppose that P_2/H is a nontrivial normal subgroup of P/H. Then $P \leq N_G(P_2)$, from which it follows that $|N_G(P_2)|_p = |P| = |N|_p$: also $|H| < |P_2|$, of course. Once again maximality of H in $\mathscr{S}$ enters the argument, forcing $N_G(P_2)$ to be p-nilpotent. This makes it clear that P_2 cannot be normal in G; since $H \leq O_p(G) \leq P$, it follows that $H = O_p(G)$.

Observe that $\bar{P} = P/H \neq 1$ since P cannot be normal in G. On applying the preceding discussion to $P_2/H = J(\bar{P})$ we obtain the p-nilpotence of $N_{\bar{G}}(J(\bar{P}))$. In a similar manner, taking P_2/H to be $\zeta(\bar{P})$ we find that $N_G(\zeta P)$ is p-nilpotent, and since $C_{\bar{G}}(\zeta\bar{P}) \leq N_G(\zeta P)/H$, the p-nilpotence of $C_{\bar{G}}(\zeta\bar{P})$ follows. Finally $|\bar{G}| < |G|$, so $\bar{G}$ is p-nilpotent by minimality of $|G|$.

In the sequel we shall write

$$K = O_{pp'}(G),$$

so that G/K is a p-group. Also a "*bar*" *will always denote a quotient group modulo* H.

(v) *P is maximal in G and $C_G(H) \leq H$.*

Since $C_G(\zeta P)$ is p-nilpotent, it is proper and lies inside a maximal subgroup M. Then $P \leq C_G(\zeta P) \leq M$, so that M is p-nilpotent by (i). We have to prove that $P = M$, or equivalently that $U \equiv O_{p'}(M) = 1$. Now $U \lhd M$ and also $H \lhd G$ and $H \leq P \leq M$, so we have $[U, H] \leq U \cap H = 1$ and $U \leq C_G(H)$. In addition $U \leq K$ because G/K is a p-group, and therefore $U \leq C_K(H)$.

Now consider $C_K(H)$. Clearly $H \cap C_K(H) = \zeta H$, from which it follows that $C_K(H)/\zeta H$ is a p'-group and ζH has a complement X in $C_K(H)$. However ζH is obviously contained in the centre of $C_K(H)$, so that in fact $C_K(H) = \zeta H \times X$. Here $X = O_{p'}(C_K(H)) \lhd G$ because $C_K(H) \lhd G$. However $O_{p'}(G) = 1$ by (ii); thus $X = 1$ and $C_K(H) = \zeta H$, a p-group. It therefore follows that $U = 1$ as required.

Finally $|C_G(H) : C_K(H)|$ is a power of p because $|G : K|$ is. Since $C_K(H) = \zeta H$ by the last paragraph, $C_G(H)$ is a p-group. Hence $C_G(H) \leq O_p(G) = H$.

(vi) *$\bar{K}$ is a nontrivial elementary abelian q-group, $q \neq p$.*

In the first place K cannot equal H, otherwise G would be a p-group and *a fortiori* p-nilpotent. Choose a prime q dividing $|K : H|$; then certainly $q \neq p$. If Q is a Sylow q-subgroup of K, the Frattini argument applies to give $G = N_G(Q)K$, from which it follows that $|G : N_G(Q)H|$ divides $|K : H|$ and is prime to p; thus $N_G(Q)H$ contains a Sylow p-subgroup of G, let us say P^g. Then $P \leq N_G(Q^{g^{-1}})H$ and, since Q may be replaced by $Q^{g^{-1}}$, we can in fact assume that $P \leq N_G(Q)H$.

Let Q_0 denote the subgroup generated by all the elements of order q in the center of Q. Since Q_0 is characteristic in Q, it is normal in $N_G(Q)$, which implies that $Q_0H \lhd N_G(Q)H$. It follows that $(Q_0H)P = Q_0P$ is a subgroup since we agreed that $P \leq N_G(Q)H$ in the last paragraph. Furthermore $G = Q_0P$ since P is maximal in G, from which we deduce that $Q = Q \cap (Q_0P) = Q_0$, thus showing Q to be elementary abelian.

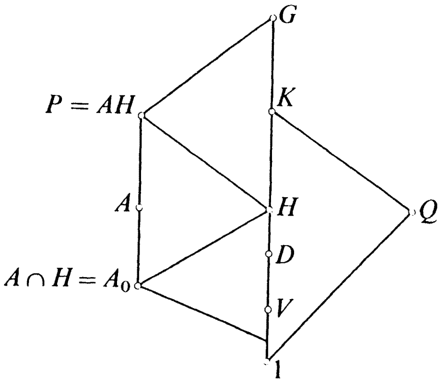
Finally $K = K \cap (QP) = Q(K \cap P) = QH$ since $K = O_{pp'}(G)$; therefore

$$K = QH \qquad \text{and} \qquad \bar{K} \simeq Q. \tag{8}$$

(vii) $C_G(\bar{K}) = K$.

Of course $C_G(\bar{K}) \geq K$ by (vi). Now $\bar{K}$ has a normal complement in $C_{\bar{G}}(\bar{K})$ a fact that shows $C_{\bar{G}}(\bar{K})$ to be the direct product of $\bar{K}$ and $P_1/H = O_p(C_{\bar{G}}(\bar{K}))$. It follows that $P_1 \lhd G$ and since P_1 is a p-group, $P_1 = H$, which yields the desired equality.

(viii) At this point one must observe that $J(P)$ cannot be contained in H; for if it were, since $H \leq P$, we should have $J(P) = J(H) \lhd G$, thus forcing $G = N_G(J(P))$ to be p-nilpotent. Consequently there is an abelian subgroup A of P with maximal rank which is not contained in H. Then $[K, A] \nleq H$; for otherwise $A \leq K$ by (vii), which would imply that $A \leq P \cap K = H$. Since $K = QH$, it follows that $[Q, A] \nleq H$.



(ix) $P = AH$ and $\bar{Q} = \bar{K}$ *is minimal normal in* $\bar{Q}\bar{A}$.

Notice that $\bar{Q} = \bar{K} \lhd \bar{G}$ and that $\bar{Q}$ is an abelian Sylow q-subgroup of $\bar{Q}\bar{A}$ in view of (vi). Applying 10.1.6 to the group $\bar{Q}\bar{A}$ we obtain a direct decomposition

$$\bar{Q} = C_{\bar{Q}}(\bar{Q}\bar{A}) \times [\bar{Q}, \bar{Q}\bar{A}] = C_{\bar{Q}}(\bar{A}) \times [\bar{Q}, \bar{A}]. \tag{9}$$

We have observed in (viii) that $[Q, A] \nleq H$; thus $[\bar{Q}, \bar{A}] \neq 1$ and we can choose Q_1 such that $Q_1 \leq Q$ and $\bar{Q}_1$ is a minimal normal subgroup of $\bar{Q}\bar{A}$ contained in $[\bar{Q}, \bar{A}]$. It is necessary to prove that $\bar{Q}_1 = \bar{Q}$.

To accomplish this we consider the subgroup

$$R = \langle H, A, Q_1 \rangle = Q_1^A AH = Q_1 AH$$

with a view to showing that it satisfies the conditions on G. We recognize AH as a Sylow p-subgroup of R: for it is surely a p-group while $AH \leq R \leq AK$ and $|AK : AH|$ is prime to p.

We shall prove first of all that $N_R(AH) = AH$. If this is false, the group AH is normalized by some element u of $Q_1 \backslash H$; this element must satisfy $[A, u] \leq (AH) \cap K$ since $u \in Q_1 \leq K$. Therefore $[A, u] \leq H$ and $uH \in C_{\bar{Q}}(\bar{A})$. This means that uH belongs to both $C_{\bar{Q}}(\bar{A})$ and $[\bar{Q}, \bar{A}]$ since $\bar{Q}_1 \leq [\bar{Q}, \bar{A}]$, which contradicts (9). Next let $x \in N_R(J(AH))$. Obviously $A \leq J(AH)$, so we have $A^x \leq J(AH) \leq AH$ and $x \in N_R(AH) = AH$. Consequently $N_R(J(AH)) = AH$, a p-group and hence certainly p-nilpotent.

Now consider $C_R(\zeta(AH))$. Since $H \leq P$, we have $\zeta P \leq C_G(H) \leq H$ by (v). Also $A \leq P$, which implies that $\zeta P \leq \zeta(AH)$ and $C_R(\zeta(AH)) \leq C_R(\zeta P)$. Since the latter is p-nilpotent, so is $C_R(\zeta(AH))$.

If $R \neq G$, the minimality of $|G|$ leads to the p-nilpotence of R; thus $R/O_{p'}(R)$ is a p-group. But $O_{p'}(R)$ centralizes H by 10.3.2 and $C_R(H) \leq H$ by (v); therefore R is a p-group and $Q_1 = 1$, which is contrary to the choice of Q_1.

Hence $G = R = Q_1 AH$, which implies that $\bar{Q} \leq \bar{Q}_1 \bar{A}$. Thus $\bar{Q} = \bar{Q}_1$, as claimed. Finally $P = AH$: for AH has been seen to be a Sylow p-subgroup of $R = G$.

(x) *$\bar{A}$ is cyclic.*

We see from (ix) that $\bar{K}$ is a simple $F_q\bar{A}$-module where $F_q = GF(q)$. Also $\bar{A}$ acts faithfully on $\bar{K}$ by (vii). Applying 9.4.3. we conclude that $\bar{A}$ is cyclic.

(xi) Write $D = \zeta H$ and consider the group QD. Obviously D is an abelian Sylow p-subgroup of QD and $D \lhd QD$. Thus 10.1.6 yields the decomposition

$$D = C_D(QD) \times [D, QD] = C_D(Q) \times [D, Q]. \qquad (10)$$

Suppose that $[D, Q] = 1$; then $Q \leq C_G(D) \leq C_G(\zeta P)$ since $\zeta P \leq C_G(H) = D$ by (v). Now $C_G(\zeta P) = P$ since P is maximal and $C_G(\zeta P)$ cannot equal G. There results the contradiction $Q = 1$, which shows that $[D, Q] \neq 1$.

Now define V as the subgroup generated by all elements of order p in $[D, Q]$. Notice that $[D, Q] = [D, QH] = [D, K] \lhd G$, so that $V \lhd G$. Of course V is an elementary abelian p-group.

(xii) $|V| \leq p^2$.

Let $A_0 = A \cap H$. Since A/A_0 is cyclic by (x), we have $r(A) - r(A_0) \leq 1$. Also $A_0 V$ is abelian because $V \leq \zeta H$. In view of $A_0 V \leq P$ and the maximality of A we have $r(A_0 V) \leq r(A)$. It is easy to show that $r(A_0 V) = r(A_0) + r(V) - r(A_0 \cap V)$, using the fact that V is elementary. Hence $r(V) - r(A_0 \cap V) \leq r(A) - r(A_0) \leq 1$. This implies that $r(V/A_0 \cap V) \leq 1$ and $V/A_0 \cap V$ is cyclic. If $1 \neq x \in Q$, then $V/A_0^x \cap V$ is cyclic, by conjugation. Now suppose that $r(V) \geq 3$; then $A_0 \cap A_0^x \cap V \neq 1$ and $I = A \cap A^x \cap V \neq 1$. If $A^x \leq P = AH$, we should have $x \in N_G(AH) = N_G(P) = P$ by maximality of P, and $x = 1$. Thus $A^x \nleq P$ and $G = \langle P, A^x \rangle = \langle H, A, A^x \rangle$, which leads to $I \leq \zeta G$. But then $I \leq C_D(Q) \cap [D, Q] = 1$ by (10), a contradiction.

(xiii) *The final step.*

We begin by showing that $C_G(V) = H$. Obviously $H \leq C_G(V) \lhd G$, and if $H \neq C_G(V)$, then $C_G(V)$ is not a p-group. Hence $Q \cap C_G(V) \neq 1$, which implies that $H < C_K(V) \leq K$. Now $C_K(V) \lhd G$ since $V \lhd G$, and yet $\bar{K}$ is a minimal normal subgroup of $\bar{Q}\bar{A}$ by (ix). Hence $K = C_K(V)$. However this yields $V \leq C_D(Q) \cap [D, Q] = 1$, which is certainly false. Consequently $C_G(V) = H$.

This result tells us that $\bar{G}$ is isomorphic with a group of automorphisms of V, and hence in view of (xii) with a subgroup of GL(2, p). Now SL(2, p) is normal and has index $p - 1$ in GL(2, p), indicating that all p-elements of GL(2, p) lie in SL(2, p). However P is maximal in G, so we may be sure that G, and hence $\bar{G}$, is generated by p-elements. Consequently $\bar{G}$ is isomorphic with a subgroup of SL(2, p).

Recall from 3.2.7 that $|\mathrm{SL}(2, p)| = (p - 1)p(p + 1)$. Thus $|\bar{K}| = q^m$ divides $(p - 1)(p + 1)$. Suppose that $q > 2$, so that q cannot divide both $p - 1$ and $p + 1$. Now $q^m \equiv 1 \bmod p$ by (ix) and 9.4.3, which implies that $q^m \geq p + 1$ and $q^m = p + 1$. Since p is an *odd prime* by hypothesis, $p + 1$ is even and $q = 2$. But an easy matrix calculation—see Exercise 10.4.2—reveals that SL(2, p) has precisely one element of order 2, namely -1_2, which is in the centre. Since $\bar{K}$ is elementary abelian, $\bar{K} \leq \zeta(\bar{G})$ and (vii) gives $K = G$ and hence $A \leq H$, contrary to the choice of A, which is our final contradiction. □

EXAMPLE. *Thompson's theorem is not true if* $p = 2$. For let $G = S_4$ and let P be a Sylow 2-subgroup. Then P is a dihedral group of order 8 and it is easy to see that for this group $J(P) = P$ and $N_G(J(P)) = P$; in addition $C_G(\zeta P) = P$. Of course P is 2-nilpotent but G does not have this property: indeed $O_{2'}(G) = 1$.

Groups with a Nilpotent Maximal Subgroup

In Chapter 9 we proved the theorem of Schmidt that a finite group whose maximal subgroups are all nilpotent is soluble. We shall use Thompson's criterion to establish a notable improvement of Schmidt's theorem which applies to groups in which a single maximal subgroup is nilpotent.

10.4.2 (Thompson). *If a finite group G has a nilpotent maximal subgroup M of odd order, then G is soluble.*

Proof. As usual we suppose the theorem false and choose for G a counter-example of smallest order. If M contains a nontrivial normal subgroup N of G, then G/N is soluble by minimality of $|G|$: therefore G is soluble, N being nilpotent. Hence the core of M in G must be 1.

Choose a prime p dividing $|M|$ and let P_0 be the unique Sylow p-subgroup of M. Then P_0 is contained in a Sylow p-subgroup P of G. Since M is

maximal and P_0 is not normal in G, it must be true that $N_G(P_0) = M$, which implies that $N_P(P_0) = P \cap M = P_0$. By the normalizer condition $P_0 = P$, which means that $|G : M|$ is prime to p and M is a Hall π-subgroup where π is the set of prime divisors of $|M|$.

We aim next to show that Thompson's theorem is applicable to G. Since $J(P)$ is characteristic in P, it is normal in M. Now $J(P)$ cannot be normal in G, so it follows that $N_G(J(P)) = M$. For exactly the same reason $C_G(\zeta P) = M$. Thus 10.4.1 assures us that G is p-nilpotent for every prime p in π. Defining L to be the intersection of all $O_{p'}(G)$ for p in π, we see that L is a π'-group and G/L a π-group. Since M is a Hall π-subgroup, it follows that $G = ML$ and $M \cap L = 1$.

Let Q be any Sylow subgroup of L. Then $G = N_G(Q)L$ by the Frattini argument. The Schur–Zassenhaus Theorem provides us with a complement of $N_L(Q)$ in $N_G(Q)$, say $N_G(Q) = XN_L(Q)$. This gives $G = XN_L(Q)L = XL$, so that X is another complement of L in G and $X = M^g$ for some g by the conjugacy part of the Schur–Zassenhaus Theorem. It follows that X is a maximal subgroup and $Q \lhd XQ = G$. Hence every Sylow subgroup of L is normal and so L is nilpotent. Since $G/L \simeq M$, it follows that G is soluble. □

In fact 10.4.2 is false if the maximal subgroup possesses elements of order 2; for the simple group PSL(2, 17) has a maximal subgroup of dihedral type D_{16}. However Deskins and Janko have proved that 10.4.2 remains true if the Sylow 2-subgroup is allowed to have class at most 2. For details see [b6].

Exercises 10.4

1. Let G be a finite group whose order is not divisible by 6. Let P be a Sylow p-subgroup of G. Prove that G is p-nilpotent if and only if $N_G(J(P))$ and $C_G(\zeta P)$ are both p-nilpotent.

2. If p is an odd prime, prove that the only element of order 2 in SL(2, p) is -1_2. Deduce that a Sylow 2-subgroup of SL(2, p) is a generalized quaternion group and that a Sylow 2-subgroup of PSL(2, p) is dihedral. [*Hint*: Apply 5.3.6.]

3. Let P be a Sylow 2-subgroup of $G =$ PSL(2, 17). Show that $P \simeq D_{16}$ and that $P = N_G(P)$. Show also that $N_G(J(P)) = P = C_G(\zeta P)$. Thus the p-nilpotence of $N_G(J(P))$ and $C_G(\zeta P)$ does not imply the solubility of G. (*Remark*: P is actually maximal in G.)

4. Assume that the finite group G has a nilpotent maximal subgroup M. If Fit $G = 1$, prove that M is a Hall π-subgroup of G for some π.

5. Let M be a maximal subgroup of a finite group G. Assume that each subgroup of M is normal in M. Prove that G cannot be simple unless its order is a prime.

10.5. Fixed-Point-Free Automorphisms

An automorphism α of a group G is said to have a *fixed point* g in G if $g^\alpha = g$; thus $C_G(\alpha)$ is the set of all fixed points of α. If $C_G(\alpha) = 1$, and 1 is the only fixed point of α, then α is called *fixed-point-free*. A *subgroup* H of Aut G is said to be fixed-point-free if every nontrivial element of H is fixed-point-free.

We shall make use of Thompson's criterion for p-nilpotency to prove an important theorem about groups with a fixed-point-free automorphism of prime order: this can then be applied to the structure of Frobenius groups.

The following lemma collects together the most elementary properties of fixed-point-free automorphisms.

10.5.1. *Let α be be a fixed-point-free automorphism of a finite group G and let α have order n.*

(i) *If $(i, n) = 1$, then α^i is also fixed-point-free.*
(ii) *The mapping $-1 + \alpha$ which sends x to $x^{-1+\alpha} = x^{-1}x^\alpha$ is a permutation of G.*
(iii) *x and x^α are conjugate if and only if $x = 1$.*
(iv) *$x^{1+\alpha+\cdots+\alpha^{n-1}} = 1$ for all x in G.*

Proof. (i) holds because α is a power of α^i.

(ii) If $x^{-1+\alpha} = y^{-1+\alpha}$, then $(xy^{-1})^\alpha = xy^{-1}$ and $x = y$. Since G is finite, $-1 + \alpha$ is a permutation.

(iii) Suppose that $x^\alpha = x^g$ for some g in G. By (ii) it is possible to write $g = y^{-1+\alpha}$ for some y in G. It follows that $x^\alpha = x^g = y^{-\alpha}(yxy^{-1})y^\alpha$ and hence that $(yxy^{-1})^\alpha = yxy^{-1}$. Therefore $yxy^{-1} = 1$ and $x = 1$.

(iv) Let $z = x^{1+\alpha+\cdots+\alpha^{n-1}}$; then $z^\alpha = x^{\alpha+\alpha^2+\cdots+\alpha^{n-1}+1} = z^x$. Thus $z = 1$ by (iii). □

10.5.2. *If α is a fixed-point-free automorphism of a finite group G, then for each prime p there is a Sylow p-subgroup P such that $P^\alpha = P$.*

Proof. Let P_0 be any Sylow p-subgroup. Then $P_0^\alpha = P_0^g$ for some g in G. Applying 10.5.1(ii), we may write $g = h^{-1+\alpha}$ for a suitable h: now let $P = P_0^{h^{-1}}$. Then

$$P^\alpha = (P_0^{h^{-1}})^\alpha = (P_0^\alpha)^{h^{-\alpha}} = (P_0^g)^{g^{-1}h^{-1}} = P_0^{h^{-1}} = P. \qquad \square$$

10.5.3. *Let H be a group of automorphisms of a finite abelian group A. Suppose that H is the semidirect product $\langle\sigma\rangle \ltimes M$ where $\sigma\beta$ is fixed-point-free of prime order p for every β in M. Assume also that $|A|$ and $|M|$ are coprime. Then $M = 1$.*

Proof. Let $a \in A$ and $\beta \in M$. Then $a^{1+\sigma\beta+\cdots+(\sigma\beta)^{p-1}} = 1$ by 10.5.1. Taking the product of these equations for all β in M and remembering that A is abelian, we obtain

$$1 = \prod_{\beta \in M} \prod_{i=0}^{p-1} a^{(\sigma\beta)^i} = a^{|M|} \prod_{i=1}^{p-1} \prod_{\beta \in M} a^{(\sigma\beta)^i}. \tag{11}$$

We claim that if i is a fixed integer satisfying $1 \leq i < p - 1$, the elements $(\sigma\beta)^i$, $\beta \in M$, are all different. For suppose that $(\sigma\beta)^i = (\sigma\bar{\beta})^i$; then $\sigma\beta \in \langle\sigma\bar{\beta}\rangle$ since $(i, p) = 1$ and $(\sigma\beta)^p = 1$. Thus $\sigma\beta = (\sigma\bar{\beta})^j$ where $1 \leq j < p$; however this implies that $j = 1$ and $\beta = \bar{\beta}$ because $\langle\sigma\rangle \cap M = 1$ and σ has order p. This establishes our claim. Hence these elements $(\sigma\beta)^i$ account for all the elements $\sigma^i\beta$, (i being fixed). Therefore

$$\prod_{\beta \in M} a^{(\sigma\beta)^i} = \prod_{\beta \in M} a^{\sigma^i\beta},$$

so that (11) yields

$$a^{-|M|} = \prod_{i=1}^{p-1} \prod_{\beta \in M} a^{\sigma^i\beta}.$$

But the right-hand side of this last equation is clearly fixed by each element of M; since $(|a|, |M|) = 1$, we deduce that a is fixed by each such element. Because a was an arbitrary element of A, we conclude that $M = 1$. □

We come now to the principal theorem of this section.

10.5.4 (Thompson). *Let G be a finite group and let p be a prime. If G has a fixed-point-free automorphism α of order p, then G is nilpotent.*

Proof. Assume that the theorem is false and let G be a counterexample of minimal order. We see from 10.5.1(ii) that $-1 + \alpha$ is surjective on $G/\zeta G$, so the hypotheses on G are inherited by $G/\zeta G$. Hence $\zeta G = 1$. The plan of attack is first to deal with the case where G is soluble, then to use Thompson's criterion to reduce the general case.

(i) *Case G soluble.*

Let $1 \neq A \lhd G$ and let A be minimal subject to $A^\alpha = A$. Since $(A')^\alpha = A'$, we see that A is abelian and, since $(A^q)^\alpha = A^q$, that A is an elementary q-group for some prime q. Now G cannot be a q-group because it is not nilpotent, so there exists a prime r different from q dividing $|G|$. Also 10.5.2 tells us that G has an α-admissible Sylow r-subgroup R. Observe that $r \neq p$ otherwise α would have a fixed point in R since $\langle\alpha\rangle \ltimes R$ would be nilpotent.

If $AR \neq G$, then, since $(AR)^\alpha = AR$, the minimality of $|G|$ forces AR to be nilpotent and thus $R \leq C_G(A)$ because $(|A|, |R|) = 1$. Should this be true for all $r \neq q$, the group $\bar{G} = G/C_G(A)$, and hence $\bar{G} \ltimes A$, would be a q-group and thus nilpotent, leading to the contradiction $A \cap \zeta G \neq 1$. Consequently $G = AR$ for some $r \neq q$.

Let σ be the restriction of α to A and let M denote the group of automorphisms of A that arise from conjugation by elements of R. Then

$H = \langle \sigma, M \rangle = \langle \sigma \rangle \ltimes M \leq \text{Aut } A$. We shall show that the conditions of 10.5.3 are met in H.

Let $g \in R$ and let $g^\tau \in M$ be the automorphism induced by conjugation by g in A. We claim that σg^τ is conjugate to σ in Aut A; this will show that σg^τ is a fixed-point-free automorphism of order p. Since α^{-1} is fixed-point-free on R, we can find an r in R such that $g^{\alpha^{-1}} = r^{-1+\alpha^{-1}}$; hence $g = r^{-\alpha+1}$. The automorphism $(r^\tau)^{-1}\sigma r^\tau$ sends $a \in A$ to $b = r^{-1}(rar^{-1})^\sigma r$. Now $(rar^{-1})^\sigma = (rar^{-1})^\alpha = r^\alpha a^\sigma r^{-\alpha}$, so that $b = r^{-1+\alpha}a^\sigma r^{-\alpha+1} = g^{-1}a^\sigma g$. Hence $(r^\tau)^{-1}\sigma r^\tau = \sigma g^\tau$ as required.

We may now apply 10.5.3 to show that $M = 1$, that is, $[A, R] = 1$. However this gives the contradiction $1 \neq A \leq \zeta G$ since $G = AR$.

(ii) *Case G insoluble.*

Let q be an odd prime dividing $|G|$. By 10.5.2 there is a Sylow q-subgroup Q such that $Q^\alpha = Q$. Hence $J(Q)^\alpha = J(Q)$, which implies that $N_G(J(Q))$ is α-admissible. If $J(Q) \lhd G$, then $G/J(Q)$ would be nilpotent and G soluble, which by (i) cannot be the case. Therefore $N_G(J(Q))$ is a proper subgroup, and, being α-admissible, it is nilpotent. For similar reasons $C_G(\zeta Q)$ is nilpotent. Thompson's criterion now shows that G is q-nilpotent and $G/O_{q'}(G)$ a q-group. Since $O_{q'}(G)$ is proper and α-admissible, it is nilpotent and G is soluble. □

In addition rather precise information is available concerning the structure of a fixed-point-free automorphism group.

10.5.5. *Let H be a fixed-point-free group of automorphisms of a finite group G. Then every subgroup of H with order pq where p and q are primes is cyclic. The Sylow p-subgroups of H are cyclic if p is odd and cyclic or generalized quaternion if* $p = 2$.

Proof. Let S be a noncyclic subgroup of H with order pq. Then by Exercise 1.6.13 there is a normal Sylow subgroup, say Q of order q, and clearly $S = QP$ where P is a subgroup of order p. By 10.5.4 the group G is nilpotent: let R be a nontrivial Sylow r-subgroup of G. Clearly $R^S = R$. Also, if $r = q$, then $Q \ltimes R$ would be nilpotent and have nontrivial center, which would prevent H from being fixed-point-free. Therefore $r \neq q$. Let $P = \langle \alpha \rangle$ and let $\beta \in Q$; then $|\alpha\beta|$ cannot equal pq since $|S| = pq$ and S is not cyclic; thus $|\alpha\beta| = p$. Now $\alpha\beta$ is fixed-point-free, so we may apply 10.5.3 to S as a group of automorphisms of ζR, obtaining at once the contradiction $[\zeta R, Q] = 1$. The structure of the Sylow subgroups is now a direct consequence of 5.3.6. □

EXAMPLE. *There is a finite nonnilpotent group with a fixed-point-free automorphism of order* 4. Let $A = \langle a \rangle \times \langle b \rangle$ be an elementary abelian 7-group of order 49, and let $X = \langle x \rangle$ be a cyclic group of order 3. The assignments $a \mapsto a^2$ and $b \mapsto b^4$ determine an automorphism of A with order 3. Thus

there is a corresponding semidirect product $G = X \ltimes A$; this is a metabelian group of order 147. One easily verifies that the assignments $a \mapsto b$, $b \mapsto a^{-1}$, $x \mapsto x^{-1}$ determine an automorphism of G with order 4. A typical element g of G will have the form $x^i a^j b^k$ where $0 \leq i < 3$ and $0 \leq j, k < 7$, and g is mapped by α to $x^{-i} b^j a^{-k}$. Thus g is a fixed point if and only if $i = j = k = 0$, that is, $g = 1$. Hence α is fixed-point-free, but G is not nilpotent.

Frobenius Groups

Recall from Chapter 8 that a group G is a *Frobenius group* if it has a proper nontrivial subgroup H such that $H \cap H^g = 1$ for all g in $G \backslash H$. By 8.5.5 there is a Frobenius kernel, that is, a normal subgroup K such that $G = HK$ and $H \cap K = 1$.

The following fundamental theorem on Frobenius groups is a consequence of the main results of this section.

10.5.6. *Let G be a finite Frobenius group with kernel K and complement H. Then:*

(i) *K is nilpotent (Thompson);*
(ii) *the Sylow p-subgroups of H are cyclic if $p > 2$ and cyclic or generalized quaternion if $p = 2$ (Burnside).*

Proof. Let $1 \neq h \in H$ and suppose that $k^h = k$ where $k \in K$. Then $1 \neq h^k = k \in H \cap H^k$, whence $k \in H \cap K = 1$ by definition of a Frobenius group. Hence conjugation by h in K induces a fixed-point-free automorphism in K. It follows immediately from 10.5.4 that K is nilpotent. Since $C_H(K) = 1$, the group H is a fixed-point-free group of automorphisms of K. The second statement is now a consequence of 10.5.5. □

Exercises 10.5

1. A finite group has a fixed-point-free automorphism of order 2 if and only if it is abelian and has odd order.
2. Let G be a finite group with a fixed-point-free automorphism α of order 3. Prove that $[x, y, y] = 1$ for all x, y in G. [For the structure of such groups see 12.3.6. *Hint*: Show first that $[x, x^\alpha] = 1$ and then prove that $[x^y, x^\alpha] = 1$ for all x, y.]
3. Let α be a fixed-point-free automorphism of a finite group G. If α has order a power of a prime p, then p does not divide $|G|$. If $p = 2$, infer via the Feit–Thompson Theorem that G is soluble.
4. If X is a nontrivial fixed-point-free group of automorphisms of a finite group G, then $X \ltimes G$ is a Frobenius group.
5. Let G be a finite Frobenius group with Frobenius kernel K. If $|G : K|$ is even, prove that K is abelian and has odd order.

6. Suppose that G is a finite group with trivial center. If G has a nonnormal abelian maximal subgroup A, prove that $G = AN$ and $A \cap N = 1$ for some elementary abelian p-subgroup N which is minimal normal in G. Show also that A must be cyclic of order prime to p. [*Hint*: Prove that $A \cap A^x = 1$ if $x \in G \backslash A$.]

7. If a finite group G has an abelian maximal subgroup, then G is soluble with derived length at most 3.

8. A finite Frobenius group has a unique Frobenius kernel, namely Fit G. Deduce that all Frobenius complements are conjugate (see Exercise 9.1.1).

9. If a finite Frobenius group G has a Frobenius complement of odd order, then G is soluble. (Do not use the Feit–Thompson Theorem.)

10. Let P be a nonabelian group of order 7^3 and exponent 7. Find a fixed-point-free automorphism of P with order 3. Hence construct a Frobenius group with nonabelian Frobenius kernel.

CHAPTER 11

The Theory of Group Extensions

The object of extension theory is to show how a group can be constructed from a normal subgroup and its quotient group. In this subject concepts from homological algebra arise naturally and contribute greatly to our understanding of it. The necessary homological machinery, including the definitions of the (co)homology groups, is presented in 11.2.

The classical theory of group extensions was developed by O. Hölder and O. Schreier while the homological implications of the theory were first recognized by S. Eilenberg and S. MacLane. Much of the version presented here is due to K.W. Gruenberg.

11.1. Group Extensions and Covering Groups

If N and G are arbitrary groups, an extension of N by G is, in familiar parlance, a group E possessing a normal subgroup M such that $M \simeq N$ and $E/M \simeq G$. For our purposes it is best to be rather more specific. By a *group extension of N by G* we shall mean a short exact sequence of groups and homomorphisms

$$1 \longrightarrow N \xrightarrow{\mu} E \xrightarrow{\varepsilon} G \longrightarrow 1.$$

The main features here are firstly that μ is injective and ε surjective, and secondly that $\operatorname{Im} \mu = \operatorname{Ker} \varepsilon = M$ say. Thus $M \simeq N$ and $E/M \simeq G$, so E is an extension of N by G in the original sense. The group N is called the *kernel* of the extension.

For the sake of brevity let us agree to write $\rightarrowtail$ to denote a monomorphism and $\twoheadrightarrow$ an epimorphism. The above extension becomes in this

notation

$$N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G.$$

Extensions of N by G always exists. For example, we may form the semi-direct product $E = G \ltimes_\xi N$ corresponding to a homomorphism $\xi: G \to \text{Aut } N$. Define $a^\mu = (1, a)$ and $(g, a)^\varepsilon = g$ where $a \in N$, $g \in G$. Then

$$N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$$

is an extension of N by G.

Morphisms of Extensions

By a *morphism* from $N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ to $\bar{N} \overset{\bar{\mu}}{\rightarrowtail} \bar{E} \overset{\bar{\varepsilon}}{\twoheadrightarrow} \bar{G}$ is meant a triple of homomorphisms (α, β, γ) such that the following diagram commutes:

$$\begin{array}{ccccc} N & \overset{\mu}{\rightarrowtail} & E & \overset{\varepsilon}{\twoheadrightarrow} & G \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\ \bar{N} & \overset{\bar{\mu}}{\rightarrowtail} & \bar{E} & \overset{\bar{\varepsilon}}{\twoheadrightarrow} & \bar{G}. \end{array}$$

We mention that the collection of all group extensions of N by G and morphisms between them is a category, although this will play no part in the sequel.

Certain types of morphisms are of special interest, foremost among them *equivalences*; these are morphisms of the form $(1, \beta, 1)$ from $N \rightarrowtail E \twoheadrightarrow G$ to $N \rightarrowtail \bar{E} \twoheadrightarrow G$. A more general type of morphism is an *isomorphism*; this is a morphism of the form $(\alpha, \beta, 1)$ from $N \rightarrowtail E \twoheadrightarrow G$ to $\bar{N} \rightarrowtail \bar{E} \twoheadrightarrow G$ where α is an isomorphism of groups. It is easy to see that β too must be an isomorphism. It is clear that equivalence and isomorphism of extensions are equivalence relations.

Couplings

Let $N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ be an extension. By choosing a transversal to $M = \text{Im } \mu = \text{Ker } \varepsilon$ in E one obtains a function $\tau: G \to E$ called a *transversal function.* Thus if $x \in E$, the coset representative of xM is $(x^\varepsilon)^\tau$. Usually τ will not be a homomorphism—a fact that makes extension theory interesting. But τ will always have the property

$$\tau\varepsilon = 1.$$

Conversely any function τ with this property determines a transversal to M in G, namely the set $\{g^\tau | g \in G\}$.

We associate with each g in G the operation of conjugation by g^τ in M. Since $M \simeq N$, this leads to an automorphism g^λ of N described by the rule

$$(a^{g^\lambda})^\mu = (g^\tau)^{-1} a^\mu (g^\tau), \qquad (a \in N, g \in G). \tag{1}$$

In this way we obtain a function $\lambda\colon G \to \operatorname{Aut} N$.

To what extent does λ depend upon the choice of transversal function τ? If τ' is another transversal function, then g^τ and $g^{\tau'}$ differ by an element of M. Consequently, if τ' leads to a function $\lambda'\colon G \to \operatorname{Aut} N$, then g^λ and $g^{\lambda'}$ differ by an inner automorphism of N, as one can see from (1). Hence $g^\lambda(\operatorname{Inn} N) = g^{\lambda'}(\operatorname{Inn} N)$, which makes it reasonable to define a function

$$\chi\colon G \to \operatorname{Out} N$$

by the rule

$$g^\chi = g^\lambda(\operatorname{Inn} N); \tag{2}$$

here χ does not depend on the transversal function. What is more, χ *is a homomorphism* because $(g_1 g_2)^\tau \equiv g_1^\tau g_2^\tau \bmod M$.

Thus each extension $N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ determines a unique homomorphism $\chi\colon G \to \operatorname{Out} N$ which arises from conjugation in $\operatorname{Im} \mu$ by elements of E. If G and N are arbitrary groups, we shall refer to a homomorphism $\chi\colon G \to \operatorname{Out} N$ as a *coupling* of G to N, whether or not it arises from an extension.

If C is the center of N, a coupling χ of G to N gives rise to a G-module† structure of C, namely $a^g = a^{g^\chi}$; this action is well-defined because $\operatorname{Inn} N$ acts trivially on C. In the very important case where N is abelian, the coupling $\chi\colon G \to \operatorname{Aut} N$ prescribes a G-module structure for N.

11.1.1. *Equivalent extensions have the same coupling.*

Proof. Let $(1, \theta, 1)$ be an equivalence from $N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ to $N \rightarrowtail \bar{E} \twoheadrightarrow G$; then there is a commutative diagram

$$\begin{array}{ccccc} N & \overset{\mu}{\rightarrowtail} & E & \overset{\varepsilon}{\twoheadrightarrow} & G \\ \| & & \downarrow{\scriptstyle\theta} & & \| \\ N & \underset{\bar{\mu}}{\rightarrowtail} & \bar{E} & \underset{\bar{\varepsilon}}{\twoheadrightarrow} & G \end{array} \tag{3}$$

(Here the left and right vertical maps are *identity functions.*) Let χ and $\bar{\chi}$ be the respective couplings of the two extensions. Choose a transversal function $\tau\colon G \to E$ for $N \rightarrowtail E \twoheadrightarrow G$. Then $\bar{\tau} = \tau\theta$ is a transversal function for the second extension: this is because $\bar{\tau}\bar{\varepsilon} = \tau(\theta\bar{\varepsilon}) = \tau\varepsilon = 1$ by commutativity of (3).

† In order to assign a $\mathbb{Z}G$-module structure to an abelian group M it is enough to prescribe the action of the elements of G. We shall therefore treat the terms "G-module" and $\mathbb{Z}G$-module" as synonymous.

Let us use τ and $\bar{\tau}$ to compute the couplings χ and $\bar{\chi}$. In the first place $g^\chi = g^\lambda(\text{Inn } N)$ and $g^{\bar{\chi}} = g^{\bar{\lambda}}(\text{Inn } N)$ where $\lambda: G \to \text{Aut } N$ and $\bar{\lambda}: G \to \text{Aut } N$ arise from τ and $\bar{\tau}$ as in (1). Applying θ to (1) and keeping in mind that $\mu\theta = \bar{\mu}$, by (3), we obtain $(a^{g^\lambda})^{\bar{\mu}} = (g^{\bar{\tau}})^{-1}a^{\bar{\mu}}(g^{\bar{\tau}}) = (a^{g^{\bar{\lambda}}})^{\bar{\mu}}$. Hence $g^\lambda = g^{\bar{\lambda}}$ and $g^\chi = g^{\bar{\chi}}$, which shows that $\chi = \bar{\chi}$. □

The principal aims of the theory of group extensions may be summarized as follows:

(i) to decide which couplings of G to N give rise to an extension of N by G;
(ii) to construct all extensions of N by G with given coupling χ;
(iii) to decide when two such extensions are equivalent (or possibly isomorphic).

We shall see that these goals can, in principle at least, be attained with the aid of cohomology.

Split Extensions

An extension $N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ is said to *split* if there exists a transversal function $\tau: G \to E$ which is a homomorphism. For example, the semidirect product extension $N \rightarrowtail G \ltimes N \twoheadrightarrow G$ is split because $g \mapsto (g, 1)$ is a transversal function which is a homomorphism.

In fact this example is entirely typical of split extensions. For suppose that $N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ splits via a homomorphism $\tau: G \to E$. Write $X = E^{\varepsilon\tau} = G^\tau$. Since $\tau\varepsilon = 1$, we have $(x^{-\varepsilon\tau}x)^\varepsilon = x^{-\varepsilon}x^\varepsilon = 1$, so that $x^{-\varepsilon\tau}x \in M = \text{Ker } \varepsilon$ and $E = XM$. In addition $X \cap M = 1$ because $x^{\varepsilon\tau} \in M$ implies that $1 = (x^{\varepsilon\tau})^\varepsilon = x^\varepsilon$. Hence $E = X \ltimes M \simeq G \ltimes N$; this shows that every split extension is a semidirect product extension.

Complements and Derivations

Consider a split extension $N \rightarrowtail E \twoheadrightarrow G$, which can without loss be taken to be a semidirect product extension; thus $E = G \ltimes N$. Recall from 9.1 that a subgroup X with the properties $XN = E$ and $X \cap N = 1$ is called a *complement* of N in E. Of course G itself—or indeed any conjugate of G—is a complement. It is an important problem to decide whether every complement is conjugate to G.

We shall show that complements of N in E correspond to certain functions from G to N known as derivations. If X is any complement, each g in G has a unique expression of the form $g = xa^{-1}$ where $x \in X$ and $a \in N$: define $\delta = \delta_X: G \to N$ by $g^\delta = a$. Thus $gg^\delta \in X$. Let $g_i \in G$, $i = 1, 2$; then X contains the element $(g_1 g_1^\delta)(g_2 g_2^\delta)$, which equals $g_1 g_2 (g_1^\delta)^{g_2} g_2^\delta$, so that the

function δ has the property

$$(g_1 g_2)^\delta = (g_1^\delta)^{g_2} g_2^\delta. \tag{4}$$

Quite generally, if N is any G-operator group, a function $\delta: G \rightarrow N$ is called a *derivation* (or 1-*cocycle*) *from G to N* if (4) holds for all g_i in G. Notice the simple consequences of (4)

$$1^\delta = 1 \quad \text{and} \quad (g^{-1})^\delta = ((g^\delta)^{g^{-1}})^{-1}. \tag{5}$$

The set of all derivations from G to N is written

$$\mathrm{Der}(G, N) \quad \text{or} \quad Z^1(G, N).$$

Thus far we have associated a derivation with each complement. Conversely, suppose that $\delta: G \rightarrow N$ is a derivation. Then there is a corresponding complement to N in G given by $X_\delta = \{gg^\delta | g \in G\}$. It follows easily from (4) and (5) that X_δ is a subgroup. Clearly $E = X_\delta N$ and $X_\delta \cap N = 1$, so X_δ is in fact a complement.

It should be apparent to the reader that $X \mapsto \delta_X$ and $\delta \mapsto X_\delta$ are inverse mappings. Thus we can state the following result.

11.1.2. *The mapping $X \mapsto \delta_X$ is a bijection from the set of all complements of N in $E = G \ltimes N$ to* Der(G, N).

Inner Derivations

Let us now assume that N is abelian, so that N is a G-module. We shall write A instead of N.

There is a natural rule of addition for derivations, namely $a^{\delta_1 + \delta_2} = a^{\delta_1} a^{\delta_2}$. It is quite routine to check that $\delta_1 + \delta_2$ is a derivation; notice however that the commutativity of A is essential here. Further, with this binary operation Der(G, A) becomes an additive abelian group.

If $a \in A$, we define a function $\delta(a): G \rightarrow A$ by the rule

$$g^{\delta(a)} = [g, a] = a^{-g+1}.$$

The commutator identity $[g_1 g_2, a] = [g_1, a]^{g_2} [g_2, a]$ tells us at once that $\delta(a)$ is a derivation. Such derivations are called *inner* (or 1-*coboundaries*), the subset of inner derivations being written

$$\mathrm{Inn}(G, A) \quad \text{or} \quad B^1(G, A)$$

Now $[g, ab^{-1}] = [g, b]^{-1} [g, a]$ since A is abelian. Therefore $\delta(ab^{-1}) = \delta(a) - \delta(b)$ and consequently Inn(G, A) is a subgroup of Der(G, A).

The significance of the inner derivations is that they determine complements which are conjugate to G.

11.1.3. *If A is a right G-module, there is a bijection between the set of conjugacy classes of complements of A in $G \ltimes A$ and the quotient group* $\mathrm{Der}(G, A)/\mathrm{Inn}(G, A)$ *in which the conjugacy class of G corresponds to* $\mathrm{Inn}(G, A)$.

Proof. Suppose that X and Y are conjugate complements. Then $X = Y^{y_1 a} = Y^a$ for some $y_1 \in Y$, $a \in A$. If $g \in G$, then $gg^{\delta_X} \in X$ where δ_X is the derivation arising from X. Then $gg^{\delta_X} = y^a$ for some y in Y. Now $y^a = y[y, a]$, so $gg^{\delta_X} = y[y, a]$, which shows that $[y, a] = [g, a] = g^{\delta(a)}$ because A is abelian. Therefore $g(g^{\delta_X} g^{-\delta(a)}) = y \in Y$. Consequently $\delta_Y = \delta_X - \delta(a)$ and $\delta_X \equiv \delta_Y$ mod($\mathrm{Inn}(G, A)$). Reversing the argument one can show that if $\delta_Y = \delta_X - \delta(a)$, then $gg^{\delta_X} = (gg^{\delta_Y})^a$, so that $X = Y^a$. This completes the proof. □

Thus all complements of A in $G \ltimes A$ are conjugate if and only if the group $\mathrm{Der}(G, A)/\mathrm{Inn}(G, A)$ is trivial. We shall see later that this quotient group can be interpreted as the first degree cohomology group $H^1(G, A)$.

Factor Sets and Extensions with Abelian Kernel

Before proceeding with the general theory of extensions we shall consider the special case of extensions with abelian kernel.

Consider an extension

$$A \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$$

where A is an abelian group, written additively; let $\chi: G \to \mathrm{Aut}\, A$ be the coupling of the extension. Then χ prescribes a G-module structure for A by conjugation; this is given by $(ax^\varepsilon)\mu = x^{-1}(a\mu)x$ where $x \in E$, $a \in A$.

As the first step in the analysis of the extension, we choose a transversal function $\tau: G \to E$; thus $\tau\varepsilon = 1$. Now τ may not be a homomorphism, but we can write for x, y in G

$$x^\tau y^\tau = (xy)^\tau((x, y)\phi)\mu,$$

where $(x, y)\phi \in A$, since $x^\tau y^\tau$ and $(xy)^\tau$ belong to the same coset of $\mathrm{Ker}\,\varepsilon = \mathrm{Im}\,\mu$. Thus we have a function

$$\phi: G \times G \to A;$$

this is subject to a restriction because of the associative law $x^\tau(y^\tau z^\tau) = (x^\tau y^\tau)z^\tau$. Substituting for products like $x^\tau y^\tau$, we obtain the fundamental equation

$$(x, yz)\phi + (y, z)\phi = (xy, z)\phi + (x, y)\phi \cdot z, \tag{6}$$

which holds for all x, y, z in G. A function $\phi: G \times G \to A$ satisfying (6) is traditionally called a *factor set*; the homological term is a *2-cocycle*, and we

shall write

$$Z^2(G, A)$$

for the set of all 2-cocycles of G with coefficients in the G-module A. Notice that $Z^2(G, A)$ has the structure of an abelian group where the group operation is defined by $(x, y)\phi_1 + \phi_2 = (x, y)\phi_1 + (x, y)\phi_2$.

The first thing we need to know is the extent to which the factor set ϕ depends on the choice of transversal function τ. Suppose that τ' is another such function for the extension $A \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$, leading to a factor set ϕ', say. Then $x^\tau y^\tau = (xy)^\tau((x, y)\phi)\mu$ and $x^{\tau'}y^{\tau'} = (xy)^{\tau'}((x, y)\phi')\mu$. Now $x^{\tau'}$ and $x^{\tau'}$ belong to the same coset of $\operatorname{Ker}\varepsilon = \operatorname{Im}\mu$. Consequently we can write $x^{\tau'} = x^\tau((x)\psi)\mu$ for some $(x)\psi \in A$. Substitute for $x^{\tau'}y^{\tau'}$ and $(xy)^{\tau'}$ in the equation defining $(x, y)\phi'$. On rearranging the terms and comparing them with the equation for $(x, y)\phi$, we quickly find that

$$(x, y)\phi = (x, y)\phi' + (xy)\psi - (x)\psi\cdot y - (y)\psi$$

for x, y, z in G. Now define $\psi^*\colon G \times G \to A$ by the rule

$$(x, y)\psi^* = (y)\psi - (xy)\psi + (x)\psi\cdot y.$$

Then $\phi' = \phi + \psi^*$, so that $\psi^* \in Z^2(G, A)$. The 2-cocycle ψ^* is of a special kind called a *2-coboundary* (n-cocycles and n-coboundaries are introduced in 11.3).

It is easy to see that the 2-coboundaries ψ^* form a subgroup of $Z^2(G, A)$: this is written

$$B^2(G, A).$$

What we have shown is that ϕ and ϕ' belong to the same coset of $B^2(G, A)$. Thus the extension determines a unique element $\phi + B^2(G, A)$ of the group

$$Z^2(G, A)/B^2(G, A).$$

This group will appear later as the cohomology group of degree 2.

Constructing Extension from Factor Sets

The next step is to start with a G-module A and a factor set $\phi\colon G \times G \to A$, and to show how to construct an extension of A by G which induces the given G-module structure of A, and which, for a suitable transversal function, has ϕ as factor set.

Let $E(\phi)$ be the set product $G \times A$. A binary operation on $E(\phi)$ is defined by the rule

$$(x, a)(y, b) = (xy, ay + b + (x, y)\phi).$$

It is straightforward to verify that this operation is associative, using the factor set condition (6). Observe that if we put $y = 1 = z$ in (6), there results $(x, 1)\phi = (1, 1)\phi$, which is therefore independent of x. Using this fact one

verifies that $(1, -(1, 1)\phi)$ is an identity element for the semigroup $E(\phi)$. Also (x, a) in $E(\phi)$ has as its inverse the element

$$(x^{-1}, -ax^{-1} - (1, 1)\phi - (x, x^{-1})\phi),$$

as one verifies using the operation on $E(\phi)$. Therefore $E(\phi)$ is a group.

Finally we can form an extension

$$A \overset{\mu}{\rightarrowtail} E(\phi) \overset{\varepsilon}{\twoheadrightarrow} G$$

by defining $a\mu = (1, a - (1, 1)\phi)$ and $(x, a)^\varepsilon = x$. For clearly $\operatorname{Ker} \varepsilon = \{(1, a) | a \in A\} = \operatorname{Im} \mu$. A simple calculation reveals that

$$(x, 0)^{-1}(1, a - (1, 1)\phi)(x, 0) = (1, ax - (1, 1)\phi)$$

(for this one needs $(1, x)\phi = (1, 1)\phi \cdot x$, and also the identity (6) with $y = x^{-1}$ and $z = x$). This equation shows that the extension induces the given G-module structure in A.

It is clear that the assignment $x \mapsto (x, 0)$ is a transversal function τ for the extension; calculating with the group operation, we find that $x^\tau y^\tau = (xy)^\tau((x, y)\phi)\mu$. Thus ϕ is indeed the factor set for the extension when the transversal function τ is used.

Equivalence

So far we have seen how to pass from extensions to factor sets and from factor sets back to extensions. Now we wish to decide when two extensions are equivalent by looking at their factor sets.

Let A be a fixed G-module and consider two extensions of A by G realizing this module structure,

$$A \overset{\mu_i}{\rightarrowtail} E_i \overset{\varepsilon_1}{\twoheadrightarrow} G, \qquad (i = 1, 2).$$

Choose transversal functions τ_i and let the resulting factor sets be ϕ_i.

First of all, suppose that the two extensions are equivalent, and that the diagram

$$\begin{array}{ccccc}
A & \overset{\mu_1}{\rightarrowtail} & E_1 & \overset{\varepsilon_1}{\twoheadrightarrow} & G \\
\Big\| & & \Big\downarrow{\scriptstyle\theta} & & \Big\| \\
A & \underset{\mu_2}{\rightarrowtail} & E_2 & \underset{\varepsilon_2}{\twoheadrightarrow} & G
\end{array}$$

commutes where θ is an isomorphism. Now $\overline{\tau_2} = \tau_1\theta$ is a transversal function for the second extension because $\overline{\tau_2}\varepsilon_2 = \tau_1\theta\varepsilon_2 = \tau_1\varepsilon_1 = 1$. Applying θ to the equation $x^{\tau_1}y^{\tau_1} = (xy)^{\tau_1}((x, y)\phi_1)\mu_1$, we obtain $x^{\overline{\tau_2}}y^{\overline{\tau_2}} = (xy)^{\tau_2}((x, y)\phi_1)\mu_2$, so that $\overline{\tau_2}$ determines the factor set ϕ_1 *for the second extension*. Therefore $\phi_1 + B^2(G, A) = \phi_2 + B^2(G, A)$ since $\overline{\tau_2}$ and τ_2 determine factor sets belonging to the same coset of $B^2(G, A)$.

Conversely, assume that $\phi_1 + B^2(G, A) = \phi_2 + B^2(G, A)$; then $\phi_1 = \phi_2 + \psi^*$ for some $\psi: G \to A$. We aim to show that the two extensions are equivalent. To this end define $\theta: E_1 \to E_2$ by

$$(x^{\tau_1}(a\mu_1))^\theta = x^{\tau_2}(a + (x)\psi)\mu_2,$$

$(x \in G, a \in A)$. Then a routine calculation shows that θ is a homomorphism. One verifies easily that $\mu_1\theta = \mu_2$—here one has to note that $1^{\tau_1} = (1, 1)\phi_1$ since $1^{\tau_1}1^{\tau_1} = 1^{\tau_1}(1, 1)\phi_1$. Finally it is clear that $\varepsilon_1 = \theta\varepsilon_2$.

It follows that θ fits into a commutative diagram

$$\begin{array}{ccccc} A & \overset{\mu_1}{\rightarrowtail} & E_1 & \overset{\varepsilon_1}{\twoheadrightarrow} & G \\ \Vert & & \downarrow{\scriptstyle\theta} & & \Vert \\ A & \underset{\mu_2}{\rightarrowtail} & E_2 & \underset{\varepsilon_2}{\twoheadrightarrow} & G. \end{array}$$

Thus θ is an isomorphism and the two extensions are equivalent. These conclusions are summarized in the following result.

11.1.4. *Let G be a group and A a G-module. Then there is a bijection between the set of equivalence classes of extensions of A by G inducing the given module structure and the group $Z^2(G, A)/B^2(G, A)$. Moreover the split extension corresponds to $B^2(G, A)$.*

In particular, every extension of A by G is equivalent to one of the constructed extensions $A \rightarrowtail E(\phi) \twoheadrightarrow G$.

This concludes our discussion of extensions with abelian kernel, which is essentially Schreier's original treatment. Next we shall show how general extensions may be constructed starting from a presentation of the quotient group.

Introduction of Covering Groups

Let N and G be given groups and let $\chi: G \to \text{Out } N$ be some coupling of G to N. We are going to show how all extensions of N by G with coupling χ—if any exist—may be constructed as images of a "covering group."

To start things off we must choose a presentation of G

$$R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} G.$$

Here, of course, F is a free group and $R = \text{Ker } \pi$. Denote by $v: \text{Aut } N \to \text{Out } N$ the natural homomorphism with kernel Inn N. By 2.1.6 a free group has the projective property; hence there is a *lifting* of $\pi\chi: F \to \text{Out } N$, that is,

a homomorphism $\xi\colon F \to \operatorname{Aut} N$ making the diagram

$$\begin{array}{ccccc} & & F & & \\ & \overset{\xi}{\swarrow} & \downarrow{\scriptstyle \pi\chi} & & \\ \operatorname{Aut} N & \xrightarrow{\ \nu\ } & \operatorname{Out} N & \longrightarrow & 1 \end{array}$$

commute. Thus $\xi\nu = \pi\chi$. Now $R^{\xi\nu} = (R^{\pi})^{\chi} = 1$, so $R^{\xi} \leq \operatorname{Ker} \nu = \operatorname{Inn} N$. Let $\bar{\xi}\colon R \to \operatorname{Aut} N$ be the restriction of ξ to R.

By the Nielson–Schreier Theorem (6.1.1) the group R is a free group. So it too has the projective property. Hence there is a homomorphism $\eta\colon R \to N$ such that $\eta\tau = \bar{\xi}$

$$\begin{array}{ccccc} & & R & & \\ & \overset{\eta}{\swarrow} & \downarrow{\scriptstyle \bar{\xi}} & & \\ N & \xrightarrow{\ \tau\ } & \operatorname{Inn} N & \longrightarrow & 1, \end{array}$$

where $\tau\colon \operatorname{Aut} N \to N$ is the conjugation homomorphism. It follows that the diagram

$$\begin{array}{ccccc} R & \rightarrowtail & F & \overset{\pi}{\twoheadrightarrow} & G \\ {\scriptstyle \eta}\downarrow & & \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \chi} \\ N & \xrightarrow{\ \tau\ } & \operatorname{Aut} N & \overset{\nu}{\twoheadrightarrow} & \operatorname{Out} N \end{array} \qquad (7)$$

is commutative.

Using the function $\xi\colon F \to \operatorname{Aut} N$, we form the semidirect product

$$S = F \ltimes_{\xi} N.$$

This is the *covering group* from whose quotient groups extensions of N by G will be formed.

11.1.5. *Let N and G be given groups, let $\chi\colon G \to \operatorname{Out} N$ be a coupling of G to N and let $R \rightarrowtail F \twoheadrightarrow G$ be a fixed presentation of G. Write $S = F \ltimes_{\xi} N$ where $\xi\colon F \to \operatorname{Aut} N$ is a lifting of χ as in (7).*

(i) *Every extension of N by G with coupling χ is equivalent to an extension $N \rightarrowtail S/M \twoheadrightarrow G$ where M is a normal subgroup of S such that $MN = M \times N = RN$.*
(ii) *Conversely every such normal subgroup M gives rise to an extension $N \rightarrowtail S/M \twoheadrightarrow G$ with coupling χ.*

Proof. Suppose first of all that $M \lhd S$ satisfies $MN = M \times N = RN$. Let $\bar{\mu}\colon N \to S/M$ and $\bar{\varepsilon}\colon S/M \to G$ be the natural mappings, $a^{\bar{\mu}} = aM$ and

$(faM)^{\bar{\varepsilon}} = f^{\pi}$, $(a \in N, f \in F)$; then there is an extension

$$N \xrightarrow{\bar{\mu}} S/M \xrightarrow{\bar{\varepsilon}} G. \tag{8}$$

For $N^{\bar{\mu}} = MN/M = RN/M = \text{Ker } \bar{\varepsilon}$. Denote the coupling of this extension by $\bar{\chi}$. To calculate $g^{\bar{\chi}}$ choose f from F so that $f^{\pi} = g$ and conjugate by f in S/M. This produces the automorphism f^{ξ} of N since $S = F \ltimes_{\xi} N$. By commutativity of (7) we have

$$g^{\bar{\chi}} = f^{\xi}(\text{Inn } N) = f^{\xi\nu} = f^{\pi\chi} = g^{\chi}.$$

Hence $\chi = \bar{\chi}$ and (8) has coupling χ. Thus (ii) has been established.

It remains to prove that an extension $N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ with coupling χ is equivalent to an extension of type (8). To establish this we begin by using once again the projective property of free groups, this time to construct a homomorphism $\gamma\colon F \to E$ such that $\gamma\varepsilon = \pi$.

$$\begin{array}{ccccc} & & F & & \\ & \swarrow^{\gamma} & \downarrow{\scriptstyle \pi} & & \\ E & \xrightarrow{\varepsilon} & G & \longrightarrow & 1. \end{array}$$

Now $(R^{\gamma})^{\varepsilon} = R^{\pi} = 1$, so $R^{\gamma} \leq \text{Ker } \varepsilon = N^{\mu}$. Thus we obtain a commutative picture

$$\begin{array}{ccccc} R & \rightarrowtail & F & \overset{\pi}{\twoheadrightarrow} & G \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \gamma} & & \| \\ N & \overset{\mu}{\rightarrowtail} & E & \overset{\varepsilon}{\twoheadrightarrow} & G \end{array} \tag{9}$$

where κ is defined by $(r^{\kappa})^{\mu} = r^{\gamma}$ and the right hand mapping is the identity function. Define x^{λ} to be the automorphism of N that arises from conjugation by x in Im μ; thus $(a^{x^{\lambda}})^{\mu} = x^{-1}a^{\mu}x$, $(a \in N, x \in E)$. Then $\lambda\colon E \to \text{Aut } N$ is surely a homomorphism. Since the coupling χ arises from conjugation in N,

$$\varepsilon\chi = \lambda\nu.$$

Therefore $\gamma\lambda\nu = (\gamma\varepsilon)\chi = \pi\chi = \xi\nu$; here we have used the commutativity of (7) and (9). Since Ker ν = Inn N, the elements $x^{\gamma\lambda}$ and x^{ξ} differ by an inner automorphism of N, say $(n_x^{\mu})^{\lambda}$, $n_x \in N$, and

$$x^{\xi} = x^{\gamma\lambda}(n_x^{\mu})^{\lambda} = (x^{\gamma}n_x^{\mu})^{\lambda} \tag{10}$$

for all $x \in E$.

Now choose a set of free generators X of F. Then there is a homomorphism $\sigma\colon F \to E$ such that $x^{\sigma} = x^{\gamma}n_x^{\mu}$ for all x in X. With this σ one has $x^{\sigma\varepsilon} = (x^{\gamma}n_x^{\mu})^{\varepsilon} = x^{\gamma\varepsilon} = x^{\pi}$ by (9). Therefore

$$\pi = \sigma\varepsilon.$$

Next we extend σ to $\sigma^*: S \to E$ by means of the rule $(fa)^{\sigma^*} = f^\sigma a^\mu$, $(f \in F$, $a \in N)$. To show that this σ^* is actually homomorphic it suffices to check that $(a^x)^{\sigma^*} = (a^{\sigma^*})^{x^{\sigma^*}}$ for all $x \in X$, $a \in N$. Now $(a^x)^{\sigma^*} = (a^x)^\mu = (a^{x^\xi})^\mu$ since $\xi: F \to \operatorname{Aut} N$ specifies the action of F on N. Further $x^\xi = (x^\gamma n_x^\mu)^\lambda = x^{\sigma\lambda}$ by (10) and the definition of σ. Thus $\xi = \sigma\lambda$. It follows that $(a^x)^{\sigma^*} = (a^{x^{\sigma\lambda}})^\mu = (x^\sigma)^{-1}a^\mu x^\sigma = (a^{\sigma^*})^{x^{\sigma^*}}$, as required.

The homomorphism $\sigma^*: S \to E$ is surjective because $E = F^\gamma N^\mu$. We shall use $M = \operatorname{Ker} \sigma^*$ to construct an extension of type (8). Suppose that $fa \in M$ where $f \in F$, $a \in N$. Then $f^\sigma \in N^\mu$ by definition of σ^*; hence $f^\pi = f^{\sigma\varepsilon} = 1$ and $f \in R$. Also $a^\mu = (f^\sigma)^{-1}$. It follows that

$$M = \{ra \mid r \in R, a \in N, a^\mu = (r^\sigma)^{-1}\}.$$

Therefore $MN = RN$. Moreover, if $ra \in M \cap N$, then $r \in F \cap N = 1$; hence $MN = M \times N$.

Defining $a^{\bar{\mu}}$ to be aM and $(faM)^{\bar{\varepsilon}}$ to be f^π we obtain an extension

$$N \overset{\bar{\mu}}{\rightarrowtail} S/M \overset{\bar{\varepsilon}}{\twoheadrightarrow} G.$$

To show that this is equivalent to the extension we started with, consider the natural isomorphism $\theta: S/M \to E$ defined by $(sM)^\theta = s^{\sigma^*}$. The diagram

$$\begin{array}{ccccc}
N & \overset{\bar{\mu}}{\rightarrowtail} & S/M & \overset{\bar{\varepsilon}}{\twoheadrightarrow} & G \\
\| & & \downarrow{\scriptstyle\theta} & & \| \\
N & \overset{\mu}{\rightarrowtail} & E & \overset{\varepsilon}{\twoheadrightarrow} & G
\end{array}$$

is commutative. For $a^{\bar{\mu}\theta} = (aM)^\theta = a^{\sigma^*} = a^\mu$ and $(faM)^{\theta\varepsilon} = (fa)^{\sigma^*\varepsilon} = (f^\sigma a^\mu)^\varepsilon = f^{\sigma\varepsilon}$; but $\sigma\varepsilon = \pi$, so $(faM)^{\theta\varepsilon} = f^\pi = (faM)^{\bar{\varepsilon}}$. This completes the proof. □

What the preceding discussion has achieved is to reduce the study of extensions to that of certain normal subgroups of covering groups. There may of course be no such normal subgroups, reflecting the fact that extensions with a prescribed coupling do not always exist. However, if N is abelian, $\operatorname{Inn} N = 1$ and $R^\xi = 1$ by (7). Thus $[R, N] = 1$ and $RN = R \times N$, so that R is a candidate for M. The corresponding extension $N \rightarrowtail S/R \twoheadrightarrow G$ is equivalent to the split extension $N \rightarrowtail G \ltimes N \twoheadrightarrow G$.

Theory of Covering Groups

We propose to study covering groups in a somewhat more general context. The outcome will be a classification of equivalence classes of extensions with given coupling.

Let there be given groups N and U together with a homomorphism $\xi\colon U \to \operatorname{Aut} N$, enabling us to form the semidirect product or *covering group*

$$S = U \ltimes_\xi N.$$

The center of N shall be denoted by C. Let V be a normal subgroup of U such that

$$[C, V] = 1.$$

The product VN is denoted by L.

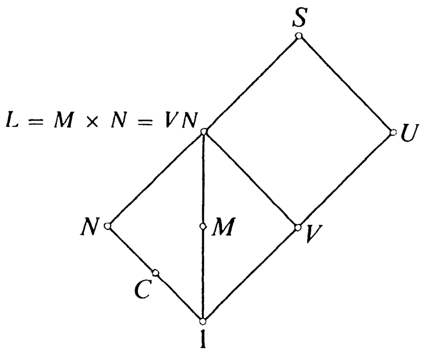
We are interested in the (possibly empty) set

$$\mathscr{M} = \mathscr{M}(U, V, N, \xi)$$

of all normal subgroups M of S with the property

$$MN = M \times N = L.$$

The relative position of these subgroups is indicated in the accompanying diagram



Each M in $\mathscr{M}$ determines an extension

$$N \overset{\mu}{\rightarrowtail} S/M \overset{\varepsilon}{\twoheadrightarrow} U/V \tag{11}$$

where $a^\mu = aM$ and $(uaM)^\varepsilon = uV$, $(a \in N, u \in U)$.

What is the relevance of this set $\mathscr{M}$ to our previous considerations? The normal subgroups M that occur in 11.1.5 are precisely the elements of $\mathscr{M}(F, R, N, \xi)$: notice that $[\zeta N, R] = 1$ because $R^\xi \leq \operatorname{Im} N$. Thus we are motivated to ask when two extensions of type (11) are equivalent.

The Action of $\operatorname{Hom}_U(V, C)$ on $\mathscr{M}$

If $\varphi \in \operatorname{Hom}_U(V, C)$, so that φ is a *U-operator homomorphism from V to C*, define $\varphi'\colon L \to L$ by the rule

$$(va)^{\varphi'} = v(av^\varphi), \qquad (v \in V, a \in N). \tag{12}$$

It is easy to check that φ' is a homomorphism using the fact that v^φ belongs to C and $[C, V] = 1$. The inverse of φ' is clearly $(-\varphi)'$, so φ' is an automorphism of L. Furthermore φ' is a U-automorphism because φ is a U-homomorphism.

Now suppose that $M \in \mathscr{M}$. Clearly $L = L^{\varphi'} = M^{\varphi'} \times N^{\varphi'} = M^{\varphi'} \times N$; also $M^{\varphi'} \lhd U$. In other words $M^{\varphi'} \in \mathscr{M}$ and $\mathrm{Hom}_U(V, C)$ acts on the set $\mathscr{M}$. Concerning this action we shall prove the following fact.

11.1.6. *If $\mathscr{M} = \mathscr{M}(U, V, N, \xi)$ is not empty, the group* $\mathrm{Hom}_U(V, C)$ *acts regularly on this set.*

Proof. Suppose first that $M^{\varphi'} = M$ where $M \in \mathscr{M}$ and $\varphi \in \mathrm{Hom}_U(V, C)$. If $\varphi' \neq 1$, then $\varphi \neq 0$, and there is an element v of V such that $v^\varphi \neq 1$. On writing $v = xa$ with $x \in M$ and $a \in N$, we see that M must contain $x^{\varphi'} = (va^{-1})^{\varphi'} = va^{-1}v^\varphi = xv^\varphi$; from this it follows that $v^\varphi \in M \cap C = 1$, a contradiction. It remains to prove transitivity.

Choose M_1 and M_2 from $\mathscr{M}$. For each v in V there are expressions $v = x_i a_i$, $i = 1, 2$, where $x_i \in M_i$, $a_i \in N$. Define a function $\varphi: V \to N$ by writing $v^\varphi = a_1 a_2^{-1}$. Now a_1 and a_2 induce the same automorphism in N as v since $[M_i, N] = 1$; hence $v^\varphi \in C$. It is obvious that φ is a homomorphism: indeed $\varphi \in \mathrm{Hom}_U(V, C)$ because $(v^u)^\varphi = a_1^u a_2^{-u} = (v^\varphi)^u$ if $u \in U$.

To complete the proof we verify that $M_1^{\varphi'} = M_2$. We choose x from M_1, writing it in the form $x = va$, $(v \in V, a \in N)$. Now $v = m_i a_i$, $i = 1, 2$, where $m_i \in M_i$, $a_i \in N$. Since $x = m_1 a_1 a$, we have $a_1 a = m_1^{-1} x \in M_1 \cap N = 1$; thus $a_1 = a^{-1}$. Consequently $x^{\varphi'} = (va)^{\varphi'} = vav^\varphi = vaa_1a_2^{-1} = m_2 \in M_2$. Hence $M_1^{\varphi'} \leq M_2$. Since $M_1^{\varphi'} \in \mathscr{M}$, it follows that $M_2 = M_2 \cap (M_1^{\varphi'} \times N) = M_1^{\varphi'}$. □

Equivalences Classes in $\mathscr{M}(U, V, N, \xi)$

In view of our interest in equivalence of group extensions the following definition is a natural one. Two elements M_1 and M_2 of $\mathscr{M}$ are said to be *equivalent* if the corresponding group extensions $N \rightarrowtail S/M_i \twoheadrightarrow U/V$, $i = 1, 2$, are equivalent. Obviously this is an equivalence relation on $\mathscr{M}$. But what are the equivalence classes? In attempting to answer this question one finds that derivations arise in an essential way.

Suppose that $\delta: U \to C$ is a derivation; denote its restriction to V by $\bar{\delta}$. Since $[V, C] = 1$, the defining property of derivations yields $(v_1 v_2)^\delta = v_1^\delta v_2^\delta$, $(v_i \in V)$; in short $\bar{\delta}: V \to C$ is a homomorphism. If $u \in U$ and $v \in V$, then by (4) and (5)

$$\begin{aligned}(u^{-1}vu)^\delta = ((u^{-1})^\delta)^{vu}(vu)^\delta &= ((u^\delta)^{u^{-1}vu})^{-1}(v^\delta)^u u^\delta \\ &= (u^\delta)^{-1}(v^\delta)^u u^\delta = (v^\delta)^u.\end{aligned}$$

It follows that $(v^u)^{\bar{\delta}} = (v^{\bar{\delta}})^u$, so that $\bar{\delta} \in \operatorname{Hom}_U(V, C)$. It should be clear to the reader that the restriction mapping $\delta \mapsto \bar{\delta}$ is a homomorphism

$$\operatorname{Der}(U, C) \to \operatorname{Hom}_U(V, C).$$

This provides us with a natural action of $\operatorname{Der}(U, C)$ on $\mathscr{M}$ in which $M^\delta = M^{\bar{\delta}'}$.

11.1.7. *If $\mathscr{M}$ is not empty, the equivalence classes of $\mathscr{M} = \mathscr{M}(U, V, N, \xi)$ are precisely the* $\operatorname{Der}(U, C)$*-orbits.*

Proof. Suppose that M_1 and M_2 are equivalent elements of $\mathscr{M}$; then there is a homomorphism θ making the diagram

$$\begin{array}{ccccc} N & \rightarrowtail & S/M_1 & \twoheadrightarrow & U/V \\ \| & & \downarrow{\scriptstyle\theta} & & \| \\ N & \rightarrowtail & S/M_2 & \twoheadrightarrow & U/V \end{array}$$

commutative. We shall find a δ in $\operatorname{Der}(U, C)$ such that $M_1^\delta = M_2$.

Let $u \in U$: then by commutativity of the right-hand square $(uM_1)^\theta$ maps to uV. Hence $(uM_1)^\theta = ucM_2$ where $c \in N$ is unique. In fact $c \in \zeta N = C$. For if $a \in N$, we have $(a^u M_1)^\theta = a^u M_2$ by commutativity of the left-hand square in the diagram; thus $a^u M_2 = ((uM_1)^\theta)^{-1}(aM_1)^\theta(uM_1)^\theta$, which becomes $a^u M_2 = a^{uc} M_2$ on substituting ucM_2 for $(uM_1)^\theta$ and aM_2 for $(aM_1)^\theta$. Hence $(a^u)^{-1} a^{uc} \in M_2 \cap N = 1$, which yields $(a^u)^c = a^u$. Since this is valid for all a in N, we conclude that $c \in C$.

The equation $(uM_1)^\theta = uu^\delta M_2$ therefore determines a function $\delta\colon U \to C$. Now θ is a homomorphism, so

$$(u_1 u_1^\delta M_2)(u_2 u_2^\delta M_2) = (u_1 u_2)(u_1 u_2)^\delta M_2,$$

which shows that $(u_1 u_2)^\delta = (u_1^\delta)^{u_2}(u_2)^\delta$—remember here that $M_2 \cap C = 1$. Thus $\delta \in \operatorname{Der}(U, C)$.

The next point to settle is that δ maps M_1 to M_2 under the action described above. Denote the restriction of δ to V by $\bar{\delta}$. If $x \in V$, then $(xM_1)^\theta = xx^\delta M_2 = x^{\bar{\delta}'} M_2$ by definition of $\bar{\delta}'$ see (12)). This also holds if $x \in N$ since in that case $(xM_1)^\theta = xM_2$ and $x^{\bar{\delta}'} = x$. Thus $(xM_1)^\theta = x^{\bar{\delta}'} M_2$ is true for all x in $L = VN$. If $x \in M_1$, it follows that $x^{\bar{\delta}'} \in M_2$ and $M_1^{\bar{\delta}'} = M_2$.

Conversely, assume that there is a δ in $\operatorname{Der}(U, C)$ such that $M_1^{\bar{\delta}'} = M_2$. Let us show that M_1 and M_2 are equivalent. Define $\theta\colon S/M_1 \to S/M_2$ by the rules $(uM_1)^\theta = uu^\delta M_2$ and $(aM_1)^\theta = aM_2$ where $u \in U$, $a \in N$. It is simple to check that $(1, \theta, 1)$ is an equivalence from $N \rightarrowtail S/M_1 \twoheadrightarrow U/V$ to $N \rightarrowtail S/M_2 \twoheadrightarrow U/V$. □

We are now able to give a description of the equivalence classes of $\mathscr{M}$.

11.1.8. *There is a bijection between the set of equivalence classes of $\mathscr{M} = \mathscr{M}(U, V, N, \xi)$ and the cokernel of the restriction homomorphism* $\text{Der}(U, C) \to \text{Hom}_U(V, C)$, *provided that $\mathscr{M}$ is not empty.*

Proof. Denote the image of the restriction map by I. Let M_0 be any fixed element of $\mathscr{M}$. If M is any other element of $\mathscr{M}$, there is a unique $\varphi_M \in \text{Hom}_U(V, C)$ such that $M = M_0^{\varphi'_M}$; this is by 11.1.6. Suppose that $\bar{M}$ is equivalent to M. Then $\bar{M} = M^{\bar{\delta}'}$ where $\delta \in \text{Der}(U, C)$ by 11.1.7. Therefore $M_0^{\varphi'_{\bar{M}}} = M_0^{\varphi'_M \bar{\delta}'} = M_0^{(\varphi_M + \bar{\delta})'}$ since $\alpha'\beta' = (\alpha + \beta)'$ by definition (12). It follows from the regularity of the action of $\text{Hom}_U(V, C)$ that $\varphi'_{\bar{M}} = (\varphi_M + \bar{\delta})'$, where $\varphi_{\bar{M}} = \varphi_M + \bar{\delta}$ or $\varphi_{\bar{M}} \equiv \varphi_M \bmod I$. Conversely this congruence implies that M and $\bar{M}$ are equivalent by reversal of the argument. □

From 11.1.5 and 11.1.8 it follows that there is a bijection between the set of equivalence classes of extensions of N by G with coupling χ and the group

$$\text{Coker}(\text{Der}(F, \zeta N) \to \text{Hom}_F(R, \zeta N)) \tag{13}$$

provided that such extensions exist: here of course $R \rightarrowtail F \twoheadrightarrow G$ is any fixed presentation of G. We shall see later that the group (13) can be identified with the second degree cohomology group $H^2(G, \zeta N)$.

Exercises 11.1

1. If (α, β, γ) is a morphism of extensions and α and γ are group isomorphisms, prove that β is an isomorphism.
2. Let $(\alpha, \theta, 1)$ be an isomorphism from $N \rightarrowtail E \twoheadrightarrow G$ to $\bar{N} \rightarrowtail \bar{E} \twoheadrightarrow G$. If these extensions have couplings χ and $\bar{\chi}$ respectively, prove that $\bar{\chi} = \chi\alpha'$ where α': Out $N \to$ Out $\bar{N}$ is induced by $\alpha: N \to \bar{N}$.
3. Let G be a group. Prove that G is free if and only if every extension by G splits. [*Hint*: Use the Nielson–Schreier Theorem.]
4. Find two isomorphic extensions of $\mathbb{Z}_3$ by $\mathbb{Z}_3 \times \mathbb{Z}_3$ which are *not* equivalent.
5. Let $A \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ be a group extension with abelian kernel A and $G = \langle g \rangle$ cyclic of order n. Let $g = x^\varepsilon$ with $x \in E$. A transversal function $\tau: G \to E$ is defined by $(g^i)^\tau = x^i$ for $0 \leq i < n$. Prove that the values of the corresponding factor set ϕ are
$$(g^i, g^j)\phi = \begin{cases} 0 & \text{if } i + j < n \\ a & \text{if } i + j \geq n \end{cases} \qquad \text{where} \quad a = x^n \in \text{Ker } \varepsilon.$$
6. Every extension $N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ is isomorphic with an extension of the form $M \overset{\iota}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ in which $M = \text{Im } \mu$ and ι is inclusion.
7. Show that there are eight equivalence classes of extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2 \times \mathbb{Z}_2$. How many nonisomorphic groups do these give rise to?

8. Let G be an infinite cyclic group and let N be any group. If $\chi: G \to \text{Out } N$ is a coupling, prove that some extension of N by G realizes χ. Using the obvious presentation $1 \rightarrowtail G \twoheadrightarrow G$, show that there is a unique equivalence class of extensions of N by G with coupling χ and that these extensions are split.

9. Let $G = \langle x \rangle$ be a cyclic group with finite order n and let N be any group. Suppose that $\chi: G \to \text{Out } N$ is a coupling that gives rise to extensions of N by G. Prove that there is a bijection between equivalence classes of extensions of N by G with coupling χ and $\text{Ker } \kappa/\text{Im } \nu$: here ν and κ are the respective endomorphisms $a \mapsto a^{1+x+\cdots x^{n-1}}$ and $a \mapsto [a, x]$ of $A = \zeta N$. (The action of x on A comes from χ.) Show also that each such extension is an image of a split extension of N by an infinite cyclic group.

10. Find all equivalence classes of extensions of Q_8 by $\mathbb{Z}_2$. Identify the groups which arise in this way.

11. Let N and G be arbitrary groups. For each x in G let N_x be a group isomorphic with N via a map $a \mapsto a_x$. Write $B = \text{Cr}_{x \in G} N_x$, the cartesian product. If $\mathbf{b} \in B$ and $g \in G$, define $\mathbf{b}^g$ by the rule $(\mathbf{b}^g)_x = b_{xg^{-1}}$. Show that this action of G on B leads to a semidirect product $W = G \ltimes B$. (Here W is called the *standard complete wreath product* $N \mathbin{\bar{\wr}} G$ and B is the *base group* of W).

12. (Kalužnin–Krasner) Let $N \overset{\mu}{\rightarrowtail} E \overset{\varepsilon}{\twoheadrightarrow} G$ be any group extension and denote by W the standard complete wreath product $N \mathbin{\bar{\wr}} G$. Prove that E is isomorphic with a subgroup of W, so that W contains an isomorphic copy of every extension of N by G. [*Hint*: Choose a transversal function $\tau: G \to E$ for the extension. Define $\gamma: E \to W$ as follows. If $x \in E$, let $x^\gamma = x^\varepsilon b(x)$ where $b(x)$ is the element of the base group of W given by $(b(x))_g = ((gx^{-\varepsilon})^\tau x (g^\tau)^{-1})^{\mu^{-1}}$.]

11.2. Homology Groups and Cohomology Groups

The purpose of this section is to define the homology and cohomology groups by means of projective resolutions. This material will be familiar to those readers who have experienced a first course in homological algebra: they may proceed directly to 11.3.

Complexes

Let R be a ring with identity. A *right R-complex* $\mathbf{C}$ is a sequence of right R-modules and homomorphisms

$$\cdots \longrightarrow C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \longrightarrow \cdots, \qquad (n \in \mathbb{Z}),$$

infinite in both directions, such that $\partial_{n+1}\partial_n = 0$, that is to say, $\text{Im } \partial_{n+1} \leq \text{Ker } \partial_n$ for all n. The *homology* $H(\mathbf{C})$ of the complex $\mathbf{C}$ is the sequence of R-modules

$$H_n\mathbf{C} = \text{Ker } \partial_n/\text{Im } \partial_{n+1}, \qquad (n \in \mathbb{Z}),$$

which are usually referred to as the *homology groups* of **C**. Thus **C** is exact if and only if all the homology groups vanish.

By a *morphism* γ from an R-complex $\mathbf{C}$ to an R-complex $\bar{\mathbf{C}}$ is meant a sequence of R-homomorphisms $\gamma_n\colon C_n \to \bar{C}_n$ such that the diagram

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \gamma_{n+1}} & & \downarrow{\scriptstyle \gamma_n} & & \downarrow{\scriptstyle \gamma_{n-1}} & & \\
\cdots & \longrightarrow & \bar{C}_{n+1} & \xrightarrow{\bar{\partial}_{n+1}} & \bar{C}_n & \xrightarrow{\bar{\partial}_n} & \bar{C}_{n-1} & \longrightarrow & \cdots
\end{array}$$

commutes. Define $\gamma_n'\colon H_n\mathbf{C} \to H_n\bar{\mathbf{C}}$ by the rule $(a + \operatorname{Im} \partial_{n+1})\gamma_n' = a\gamma_n + \operatorname{Im} \bar{\partial}_{n+1}$ where $a \in \operatorname{Ker} \partial_n$. Notice that $a\gamma_n \in \operatorname{Ker} \bar{\partial}_n$ because $a\gamma_n\bar{\partial}_n = a\partial_n\gamma_{n-1} = 0$ by commutativity of the diagram; also γ_n' is well-defined since $(\operatorname{Im} \partial_{n+1})\gamma_n = \operatorname{Im}(\gamma_{n+1}\bar{\partial}_{n+1}) \leq \operatorname{Im} \bar{\partial}_{n+1}$. Clearly γ_n' is an R-homomorphism. We state this basic observation as a lemma.

11.2.1. *A morphism* $\gamma\colon \mathbf{C} \to \bar{\mathbf{C}}$ *of R-complexes induces homomorphisms* $\gamma_n'\colon H_n\mathbf{C} \to H_n\bar{\mathbf{C}}$ *of homology groups.*

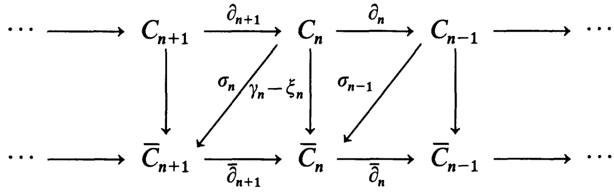
It is clear how to define a *left R-complex* of left R-modules. Most results will be proved for right complexes, but they are, of course, valid for left complexes by corresponding proofs.

Homotopy

We wish to introduce a way of comparing morphisms between complexes $\mathbf{C}$ and $\bar{\mathbf{C}}$. Two such morphisms γ and ξ are said to be *homotopic* if there exist R-homomorphisms $\sigma_n\colon C_n \to \bar{C}_{n+1}$ such that

$$\gamma_n - \xi_n = \sigma_n\bar{\partial}_{n+1} + \partial_n\sigma_{n-1}$$

for all $z \in \mathbb{Z}$. This may be thought of as a sort of partial commutativity of the diagram



—check the commutativity statements for the two middle triangles. It is very easy to verify that homotopy is an equivalence relation.

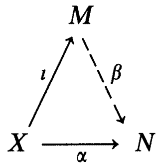
The following fact plays a central role in the proof of the uniqueness of homology and cohomology groups.

11.2.2. *If γ: $\mathbf{C} \to \overline{\mathbf{C}}$ and ξ: $\overline{\mathbf{C}} \to \mathbf{C}$ are morphisms of R-complexes such that $\gamma\xi$ and $\xi\gamma$ are homotopic to identity morphisms, then γ_n': $H_n\mathbf{C} \to H_n\overline{\mathbf{C}}$ is an isomorphism for all integers n.*

Proof. By hypothesis there are R-homomorphisms σ_n: $C_n \to C_{n+1}$ such that $\gamma_n\xi_n - 1 = \sigma_n\partial_{n+1} + \partial_n\sigma_{n-1}$. If $a \in \operatorname{Ker} \partial_n$, then $a\gamma\xi = a + a\sigma_n\partial_{n+1} \equiv a \bmod \operatorname{Im} \partial_{n+1}$. Therefore $a\gamma\xi + \operatorname{Im} \partial_{n+1} = a + \operatorname{Im} \partial_{n+1}$, which is just to say that $\gamma_n'\xi_n' = 1$. Similarly $\xi_n\gamma_n' = 1$, so that ξ_n' is the inverse of γ_n'. □

Free and Projective Modules

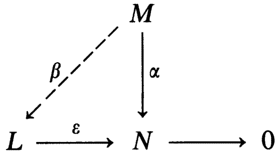
Free R-modules are defined in exactly the same way as free abelian groups, or free groups for that matter. An R-module M is said to be *free on a set* X if there is a mapping ι: $X \to M$ such that, given a function α: $X \to N$ with N any R-module, there is a unique homomorphism β: $M \to N$ such that $\alpha = \iota\beta$. Thus the diagram



commutes. The mapping ι is necessarily injective: usually we take it to be inclusion, so that $X \subseteq M$.

The following statements are proved in precisely the same way as for abelian groups: *a right R-module is free if and only if it is a direct sum of copies of* R_R, the ring R regarded as a right R-module by multiplication. *Every R-module is an image of a free-module* (see 2.3.8 and 2.3.7).

An R-module M is said to be *projective* if, given an R-homomorphism α: $M \to N$ and an R-epimorphism ε: $L \to N$, there is an R-homomorphism β: $M \to L$ such that $\alpha = \beta\varepsilon$, that is to say, the diagram



commutes. *Every free module is projective* (see the proof of 4.2.4). A projective module is not in general free, but merely a direct summand of a free module (see Exercise 11.2.6).

A complex is said to be *free* if all of its modules are free, and *projective* if all of its modules are projective.

Resolutions

A complex $\mathbf{C}$ is called *positive* if $C_n = 0$ for $n < 0$: the complex is then written $\cdots \to C_2 \to C_1 \to C_0 \to 0$. Let M be a right R-module. By a *right R-resolution* of M is meant a positive right R-complex $\mathbf{C}$ and an epimorphism $\varepsilon: C_0 \twoheadrightarrow M$ such that

$$\cdots \longrightarrow C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

is exact. We may abbreviate the resolution to $\mathbf{C} \overset{\varepsilon}{\twoheadrightarrow} M$. The resolution is said to be *free* (*projective*) if $\mathbf{C}$ is free (projective).

11.2.3. *Every R-module has a free R-resolution.*

Proof. Let M be any R-module. Then there exists an epimorphism $\varepsilon: C_0 \twoheadrightarrow M$ with C_0 is free. Likewise there exists a homomorphism $\partial_1: C_1 \to C_0$ where $\operatorname{Im} \partial_1 = \operatorname{Ker} \varepsilon$ and C_1 is free. So far we have an exact sequence $C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\varepsilon} M \to 0$. Clearly this procedure can be repeated indefinitely to produce a free resolution of M. □

11.2.4. *Let $\mathbf{P} \overset{\varepsilon}{\twoheadrightarrow} M$ and $\bar{\mathbf{P}} \overset{\bar{\varepsilon}}{\twoheadrightarrow} \bar{M}$ be two projective R-resolutions. If $\alpha: M \to \bar{M}$ is an R-homomorphism, there is a morphism $\pi: \mathbf{P} \to \bar{\mathbf{P}}$ such that $\pi_0 \bar{\varepsilon} = \varepsilon\alpha$. Moreover any two such π's are homotopic.*

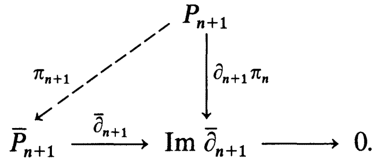
$$\begin{array}{ccc} \mathbf{P} & \overset{\varepsilon}{\twoheadrightarrow} & M \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \alpha} \\ \bar{\mathbf{P}} & \overset{\bar{\varepsilon}}{\twoheadrightarrow} & \bar{M}. \end{array}$$

Proof. Since P_0 is projective and $\bar{\varepsilon}$ surjective, there is a homomorphism $\pi_0: P_0 \to \bar{P}_0$ such that $\pi_0 \bar{\varepsilon} = \varepsilon\alpha$.

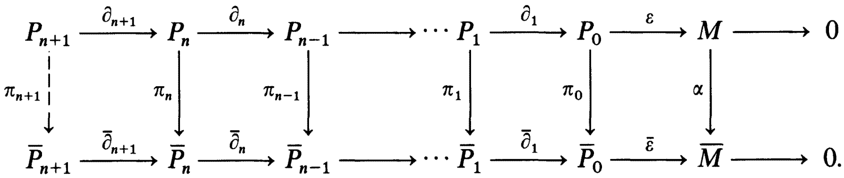
$$\begin{array}{ccccc} & & P_0 & & \\ & {\scriptstyle \pi_0}\swarrow & \downarrow{\scriptstyle \varepsilon\alpha} & & \\ \bar{P}_0 & \xrightarrow{\bar{\varepsilon}} & \bar{M} & \longrightarrow & 0. \end{array}$$

Suppose that we have constructed homomorphisms $\pi_i: P_i \to \bar{P}_i$, for $i = 1, 2, \ldots, n$, such that $\pi_i \bar{\partial}_i = \partial_i \pi_{i-1}$. Then we have $\partial_{n+1}\pi_n\bar{\partial}_n = \partial_{n+1}\partial_n\pi_{n-1} = 0$, so that $\operatorname{Im}(\partial_{n+1}\pi_n) \subseteq \operatorname{Ker} \bar{\partial}_n = \operatorname{Im} \bar{\partial}_{n+1}$. By projectivity of P_{n+1} there exists a homomorphism $\pi_{n+1}: P_{n+1} \to \bar{P}_{n+1}$ such that $\pi_{n+1}\bar{\partial}_{n+1} = \partial_{n+1}\pi_n$, as one can

see from the diagram

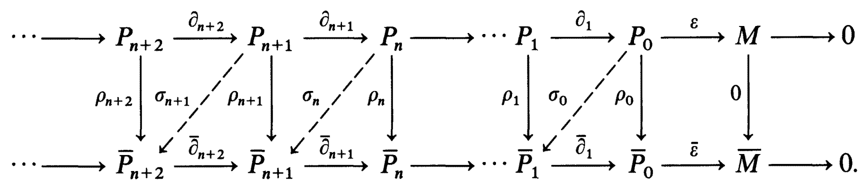


Hence the following diagram is commutative:



Consequently we have defined recursively a morphism $\pi: \mathbf{P} \to \overline{\mathbf{P}}$ with the right property.

Now suppose that $\pi': \mathbf{P} \to \overline{\mathbf{P}}$ is another such morphism. Let $\rho: \mathbf{P} \to \overline{\mathbf{P}}$ be the morphism given by $\rho_n = \pi_n - \pi'_n$. Then the following diagram commutes —ignore the diagonal maps for the present:



Since $\rho_0 \bar{\varepsilon} = 0$, we have $\operatorname{Im} \rho_0 \leq \operatorname{Ker} \bar{\varepsilon} = \operatorname{Im} \bar{\partial}_1$. By projectivity of P_0 there exists a homomorphism $\sigma_0: P_0 \to \overline{P}_1$ such that $\sigma_0 \bar{\partial}_1 = \rho_0$. Suppose that homomorphisms $\sigma_i: P_i \to \overline{P}_{i+1}$ have been constructed in such a way that $\rho_i = \partial_i \sigma_{i-1} + \sigma_i \bar{\partial}_{i+1}$ for $i = 0, 1, \ldots, n$. (Refer now to the diagram.) This is true when $i = 0$ if we interpret σ_{-1} as 0. Now

$$\begin{aligned}(\rho_{n+1} - \partial_{n+1}\sigma_n)\bar{\partial}_{n+1} &= \partial_{n+1}\rho_n - \partial_{n+1}\sigma_n\bar{\partial}_{n+1} \\ &= \partial_{n+1}(\partial_n\sigma_{n-1} + \sigma_n\bar{\partial}_{n+1}) - \partial_{n+1}\sigma_n\bar{\partial}_{n+1} \\ &= 0.\end{aligned}$$

Hence $\operatorname{Im}(\rho_{n+1} - \partial_{n+1}\sigma_n) \leq \operatorname{Ker} \bar{\partial}_{n+1} = \operatorname{Im} \bar{\partial}_{n+2}$. The projectivity of P_{n+1} yields a homomorphism $\sigma_{n+1}: P_{n+1} \twoheadrightarrow \overline{P}_{n+2}$ such that $\sigma_{n+1}\bar{\partial}_{n+2} = \rho_{n+1} - \partial_{n+1}\sigma_n$, or $\rho_{n+1} = \partial_{n+1}\sigma_n + \sigma_{n+1}\bar{\partial}_{n+2}$ as required. Thus the σ_n have been constructed for all n, and π and π' are homotopic by definition. □

The Homology Groups $H_n(G, M)$

Let G be any group and M any right G-module (that is to say, right $\mathbb{Z}G$-module). Consider the additive group of integers $\mathbb{Z}$ regarded as a trivial *left*

G-module; this means that elements of G operate on $\mathbb{Z}$ like the identity map. By 11.2.3 there is a *left* projective resolution $\mathbf{P} \to \mathbb{Z}$. By tensoring each module of $\mathbf{P}$ with M over $\mathbb{Z}G$ and taking the natural induced maps we obtain a complex of $\mathbb{Z}$-modules

$$\cdots \longrightarrow M \otimes_{\mathbb{Z}G} P_{n+1} \xrightarrow{\partial'_{n+1}} M \otimes_{\mathbb{Z}G} P_n \xrightarrow{\partial'_n} M \otimes_{\mathbb{Z}G} P_{n-1} \longrightarrow \cdots$$

which we call $M \otimes_{\mathbb{Z}G} \mathbf{P}$: here of course $(a \otimes b)\partial'_n = a \otimes (b\partial_n)$, $a \in M$, $b \in P_n$. This complex will usually not be exact. Define the nth *homology group of G with coefficients in M* to be the abelian group

$$H_n(G, M) = H_n(M \otimes_{\mathbb{Z}G} \mathbf{P}).$$

Since $\mathbb{Z}$ has many projective resolutions, the following remark is essential.

11.2.5. *Up to isomorphism the homology groups $H_n(G, M)$ are independent of the projective resolution $\mathbf{P} \to \mathbb{Z}$.*

Proof. Let $\mathbf{P} \xrightarrow{\varepsilon} \mathbb{Z}$ and $\bar{\mathbf{P}} \xrightarrow{\bar{\varepsilon}} \mathbb{Z}$ be two left projective $\mathbb{Z}G$-resolutions of $\mathbb{Z}$. Applying 11.2.4 with $1: \mathbb{Z} \to \mathbb{Z}$ for α, we obtain a morphism $\pi: \mathbf{P} \to \bar{\mathbf{P}}$ such that $\pi_0\bar{\varepsilon} = \varepsilon$. Similarly there is a morphism $\bar{\pi}: \bar{\mathbf{P}} \to \mathbf{P}$ such that $\bar{\pi}_0\varepsilon = \bar{\varepsilon}$. Then $\pi\bar{\pi}: \mathbf{P} \to \mathbf{P}$ has the property $(\pi_0\bar{\pi}_0)\varepsilon = \varepsilon$; of course so does the identity morphism $1: \mathbf{P} \to \mathbf{P}$. It follows from 11.2.4 that $\pi\bar{\pi}$ is homotopic to 1; the same is true of $\bar{\pi}\pi$. We deduce that $\pi'\bar{\pi}'$ and $\bar{\pi}'\pi'$ are homotopic to identity morphisms where $\pi': M \otimes_{\mathbb{Z}G} \mathbf{P} \to M \otimes_{\mathbb{Z}G} \bar{\mathbf{P}}$ and $\bar{\pi}': M \otimes_{\mathbb{Z}G} \bar{\mathbf{P}} \to M \otimes_{\mathbb{Z}G} \mathbf{P}$ are the natural induced morphisms in which $(a \otimes b)\pi'_n = a \otimes (b\pi_n)$ and $(a \otimes b)\bar{\pi}'_n = a \otimes (b\pi_n)$. Finally 11.2.2 shows that the map π'_n induces an isomorphism

$$H_n(M \otimes_{\mathbb{Z}G} \mathbf{P}) \to H_n(M \otimes_{\mathbb{Z}G} \bar{\mathbf{P}}). \qquad \square$$

The Cohomology Groups $H^n(G, M)$

Let G be any group and M any *right* G-module. Let $\mathbf{P} \xrightarrow{\varepsilon} \mathbb{Z}$ be a *right* projective $\mathbb{Z}G$-resolution of $\mathbb{Z}$. Form the new complex $\mathrm{Hom}_G(\mathbf{P}, M)$, that is,

$$\cdots \longrightarrow \mathrm{Hom}_G(P_{n-1}, M) \xrightarrow{\delta^n} \mathrm{Hom}_G(P_n, M) \xrightarrow{\delta^{n+1}} {}^{\mathrm{Hom}}{}_G(P_{n+1}, M) \longrightarrow \cdots$$

where δ^n is defined in the natural way, by composition; thus $(\alpha)\delta^n = \partial_n\alpha$ where $\alpha \in \mathrm{Hom}_G(P_{n-1}, M)$. Each $\mathrm{Hom}_G(P_n, M)$ is a $\mathbb{Z}$-module. Now the complex $\mathrm{Hom}_G(\mathbf{P}, M)$ will usually be inexact. The nth *cohomology group of G with coefficients in M* is the abelian group

$$H^n(G, M) = H_n(\mathrm{Hom}_G(\mathbf{P}, M)).$$

Just as for homology we can prove independence of the resolution.

11.2.6. *Up to isomorphism the cohomology groups $H^n(G, M)$ are independent of the projective resolution $\mathbf{P} \twoheadrightarrow M$.*

When a projective resolution of $\mathbb{Z}$ is known, the homology and cohomology groups may be read off from the following result.

11.2.7. *Let G be a group and M a G-module. Suppose that $\mathbf{P} \twoheadrightarrow \mathbb{Z}$ is a projective $\mathbb{Z}G$-resolution of $\mathbb{Z}$, and denote* $\operatorname{Im}(\partial_n: P_n \to P_{n-1})$ *by J_n.*

(i) *If $\mathbf{P}$ is a left complex and M is a right G-module, there is an exact sequence*

$$0 \longrightarrow H_n(G, M) \longrightarrow M \otimes_{\mathbb{Z}G} J_n \longrightarrow M \otimes_{\mathbb{Z}G} P_{n-1}.$$

(ii) *If $\mathbf{P}$ is a right complex and M is a right G-module, there is an exact sequence*

$$\operatorname{Hom}_G(P_{n-1}, M) \longrightarrow \operatorname{Hom}_G(J_n, M) \longrightarrow H^n(G, M) \longrightarrow 0.$$

Proof. (i) Let $\nu: P_n \to J_n$ be the obvious mapping $a \mapsto a\partial_n$, and let $\iota: J_n \to P_{n-1}$ be inclusion. Then we have the commutative picture with an exact row

$$\begin{array}{ccccccc} P_{n+1} & \xrightarrow{\partial_{n+1}} & P_n & \xrightarrow{\nu} & J_n & \longrightarrow & 0 \\ & & & \searrow^{\partial_n} \quad \swarrow_{\iota} & & & \\ & & & P_{n-1}. & & & \end{array}$$

Tensor each module with M, keeping in mind the right exactness property of tensor products. We obtain an induced commutative diagram with an exact row.

$$\begin{array}{ccccccc} M \otimes_{\mathbb{Z}G} P_{n+1} & \xrightarrow{\partial'_{n+1}} & M \otimes_{\mathbb{Z}G} P_n & \xrightarrow{\nu'} & M \otimes_{\mathbb{Z}G} J_n & \longrightarrow & 0 \\ & & & \searrow^{\partial'_n} \quad \swarrow_{\iota'} & & & \\ & & & M \otimes_{\mathbb{Z}G} P_{n-1}. & & & \end{array}$$

Thus $\operatorname{Ker} \nu' = \operatorname{Im} \partial'_{n+1}$. We claim that $(\operatorname{Ker} \partial'_n)\nu' = \operatorname{Ker} \iota'$. If $a \in \operatorname{Ker} \partial'_n$, then $0 = a\partial'_n = a\nu'\iota'$ by commutativity of the second diagram. Thus $a\nu' \in \operatorname{Ker} \iota'$. Conversely let $b \in \operatorname{Ker} \iota'$ and write $b = c\nu'$ where $c \in M \otimes_{\mathbb{Z}G} P_n$. Then $0 = b\iota' = c\nu'\iota' = c\partial'_n$, so $c \in \operatorname{Ker} \partial'_n$ and $b \in (\operatorname{Ker} \partial'_n)\nu'$. Hence ν' induces an isomorphism from $\operatorname{Ker} \partial'_n / \operatorname{Im} \partial'_{n+1}$ to $\operatorname{Ker} \iota'$. But $H_n(G, M) = \operatorname{Ker} \partial'_n / \operatorname{Im} \partial'_{n+1}$, so we obtain an isomorphism of $H_n(G, M)$ with

$$\operatorname{Ker}(\iota': M \otimes_{\mathbb{Z}G} J_n \longrightarrow M \otimes_{\mathbb{Z}G} P_{n-1}),$$

as called for.

(ii) The proof is similar. □

Remark: *Left modules versus right modules*

It is also possible to define $H_n(G, M)$ as $H_n(\mathbf{P} \otimes M)$ where $\mathbf{P}$ is a *right* projective resolution and M is a *left* module. Similarly $H^n(G, M)$ may be

defined to be $H_n(\text{Hom}(\mathbf{P}, M))$ where $\mathbf{P}$ is a *left* projective resolution and M is a *left* module. Up to isomorphism the same groups are obtained. The basis for this is the fact that any left module A over a group G can be regarded as a right module A' over G by means of the rule $ag = g^{-1}a$ $(a \in A, g \in G)$; for details see Exercises 11.2.10 and 11.2.11.

EXERCISES 11.2

(In the first five exercises R is a ring with identity.)

*1. Prove that a right R-module is free if and only if it is a direct sum of copies of R_R.

*2. Any R-module is an image of a free R-module.

*3. Free modules are projective.

4. Consider an *extension* of R-modules, that is, an exact sequence of R-modules and R-homomorphisms $0 \to A \xrightarrow{\mu} B \xrightarrow{\varepsilon} C \to 0$.
   (a) Prove that there is an R-homomorphism $\gamma: C \to B$ such that $\gamma\varepsilon = 1$ if and only if $\text{Im } \mu = \text{Ker } \varepsilon$ is a direct summand of B.
   (b) Prove that there is an R-homomorphism $\beta: B \to A$ such that $\mu\beta = 1$ if and only if $\text{Im } \mu = \text{Ker } \varepsilon$ is a direct summand of B.
   (The extension is said to *split* if these equivalent properties hold.)

5. Prove that the following properties of an R-module M are equivalent:
   (a) M is projective.
   (b) Every extension $0 \to A \to B \to M \to 0$ splits.
   (c) M is a direct summand of a free R-module.

6. Use Exercise 11.2.5 to give an example of a projective module that is not free.

7. If R is a principal ideal domain, prove that every projective R-module is free.

8. Let M be a free G-module and let $H \leq G$. Prove that M is a free H-module.

9. Prove 11.2.6.

10. Prove 11.2.7(ii).

11. Let $\mathbf{P}$ be a right G-complex and let M be a left G-module. If A is a left (right) G-module, let A' be the corresponding right (left) G-module where $ag = g^{-1}a$ (or $ga = ag^{-1}$). Prove that $H_n(\mathbf{P} \otimes_{\mathbb{Z}G} M) \simeq H_n(M' \otimes_{\mathbb{Z}G} \mathbf{P}')$ where $\mathbf{P}'$ is the complex whose modules are P_n'.

12. If $\mathbf{P}$ is a left G-complex and M is a left G-module, prove that $H_n(\text{Hom}_{\mathbb{Z}G}(\mathbf{P}, M)) \simeq H_n(\text{Hom}_{\mathbb{Z}G}(\mathbf{P}', M'))$ in the notation of the previous exercise.

11.3. The Gruenberg Resolution

Naturally 11.2.7 is of little value until we have some explicit method of writing down a projective $\mathbb{Z}G$-resolution of $\mathbb{Z}$. There is a way of doing this whenever a presentation of the group G is given.

Augmentation Ideals

Let G be any group. Then there is an obvious epimorphism of abelian groups

$$\varepsilon: \mathbb{Z}G \to \mathbb{Z}$$

such that $g \mapsto 1$ for all g in G: this is known as the *augmentation* of $\mathbb{Z}G$. It is easy to check that ε is a ring homomorphism. Thus the kernel of ε is an ideal of $\mathbb{Z}G$; this ideal, which is of great importance, is denoted by

$$I_G,$$

the *augmentation ideal* of $\mathbb{Z}G$. Obviously I_G consists of all $r = \sum_{g \in G} n_g g$ such that $\sum_{g \in G}(n_g) = 0$. Now such an r can be rewritten in the form $r = \sum_{1 \neq g \in G} n_g(g - 1)$; conversely any such r has coefficient sum equal to 0, so it belongs to I_G. Thus

$$I_G = \langle g - 1 \mid 1 \neq g \in G \rangle,$$

the *additive group* generated by all the $g - 1 \neq 0$. Indeed it is easy to see that I_G is a free abelian group with the set $\{g - 1 \mid 1 \neq g \in G\}$ as basis.

The following property of the augmentation ideal of a free group is fundamental.

11.3.1. *If F is a free group on a set X, then I_F is free as a right F-module on the set $\bar{X} = \{x - 1 \mid x \in X\}$.*

Proof. Let $\alpha: \bar{X} \to M$ be a mapping to some F-module M. By definition of a free module it suffices to prove that α extends to an F-homomorphism $\beta: I_F \to M$.

First of all let $\alpha': F \to F \ltimes M$ be the group homomorphism which sends x in X to $(x, (x - 1)\alpha)$. To each f in F there correspond f_1 in F and a in M such that $f^{\alpha'} = (f_1, a)$. Now it is clear from the definition of α' that $f_1 = f$. Thus a function $\delta: F \to M$ is determined by the equation $f^{\alpha'} = (f, f^{\delta})$. Next for any f_1, f_2 in F we have

$$(f_1 f_2)^{\alpha'} = f_1^{\alpha'} f_2^{\alpha'} = (f_1, f_1^{\delta})(f_2, f_2^{\delta}) = (f_1 f_2, (f_1^{\delta})f_2 + f_2^{\delta}),$$

in view of the additive nature of M. Hence $(f_1 f_2)^{\delta} = (f_1^{\delta})f_2 + f_2^{\delta}$, so that $\delta: F \to M$ is a derivation.

Keeping in mind that I_F is free as an abelian group on the set $\{f - 1 \mid 1 \neq f \in F\}$, we construct a homomorphism $\beta: I_F \to M$ of abelian groups by writing $(f - 1)\beta = f^{\delta}$. Now $(x - 1)\beta = x^{\delta} = (x - 1)\alpha$ because $x^{\alpha'} = (x, (x - 1)\alpha)$; thus β is an extension of α to I_F. Finally β is an F-homomorphism because

$$\begin{aligned}((f - 1)f_1)\beta = ((ff_1 - 1) - (f_1 - 1))\beta &= (ff_1 - 1)\beta - (f_1 - 1)\beta \\ &= (ff_1)^{\delta} - f_1^{\delta} = (f^{\delta})f_1 \\ &= (f - 1)\beta f_1.\end{aligned}$$

□

As an application of 11.3.1 let us prove that the homology and cohomology groups of a free group vanish in dimensions greater than 1.

11.3.2. *If F is a free group and M is any F-module, then $H^n(F, M) = 0 = H_n(F, M)$ for all $n > 1$.*

Proof. By 11.3.1 the complex $\cdots \to 0 \to 0 \to I_F \to \mathbb{Z}F \overset{\varepsilon}{\twoheadrightarrow} \mathbb{Z}$ is a free $\mathbb{Z}F$-resolution of $\mathbb{Z}$. Using this resolution and the definitions of $H_n(F, M)$ and $H^n(F, M)$ we obtain the result. □

Relative Augmentation Ideals

Let G be any fixed group and suppose that N is a normal subgroup of G. The assignment $g \mapsto gN$ determines an epimorphism of abelian groups from $\mathbb{Z}G$ to $\mathbb{Z}(G/N)$ which is easily seen to be a ring homomorphism. Let its kernel be denoted by

$$\bar{I}_N.$$

This may be thought of as a generalization of the augmentation ideal since $\bar{I}_G = I_G$.

Let I denote the ideal $I_N(\mathbb{Z}G) = (\mathbb{Z}G)I_N$; then clearly $I \leq \bar{I}_N$. We regard $\mathbb{Z}G/I$ as a G-module via right multiplication. If $x \in N$, $g \in G$ and $r \in \mathbb{Z}G$, then $(r + I)gx = rg + I$ since $x - 1 \in I$. We may therefore turn $\mathbb{Z}G/I$ into a G/N-module via the rule $(r + I)gN = rg + I$. It follows that $\bar{I}_N$ must act trivially on $\mathbb{Z}G/I$, or $\bar{I}_N \leq I$. There results the equalities

$$\bar{I}_N = I_N(\mathbb{Z}G) = (\mathbb{Z}G)I_N.$$

Hence $\bar{I}_N$ is the right ideal of $\mathbb{Z}G$ generated by all $x - 1$ where $1 \neq x \in N$.

The next result generalizes 11.3.1.

11.3.3. *Let R be a normal subgroup of a free group F. If R is free on X, then $\bar{I}_R$ is free as a right F-module on $\{x - 1 | x \in X\}$.*

Proof. Suppose that $\sum_{x \in X}(x - 1)a_x = 0$ where $a_x \in \mathbb{Z}F$. Choose a transversal T to R in F; then $\mathbb{Z}F = \mathrm{Dr}_{t \in T}(\mathbb{Z}R)t$, so we may write $a_x = \sum_{t \in T} b_{x,t}t$ where $b_{x,t} \in \mathbb{Z}R$. Hence $\sum_{t \in T}(\sum_{x \in X}(x - 1)b_{x,t})t = 0$. Obviously this means that $\sum_{x \in X}(x - 1)b_{x,t} = 0$ for every t. Since I_R is free on the set of all $x - 1$ by 11.3.1, it follows that $b_{x,t} = 0$. □

One final preparatory lemma is needed.

11.3.4. *Let $R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} G$ be a presentation of a group G. Suppose that S and T are right ideals of $\mathbb{Z}F$ that are free as F-modules on X and Y respectively. Then:*

(i) *$S/S\bar{I}_R$ is free as a G-module on $\{x + S\bar{I}_R | x \in X\}$;*
(ii) *ST is free as an F-module on $\{xy | x \in X, y \in Y\}$ provided that T is a 2-sided ideal.*

Proof. (i) In the first place $S/\bar{I}_R$ is a G-module via the action $(s + S\bar{I}_R)f^\pi = sf + S\bar{I}_R$; this is well-defined because $srf = sf + s(r-1)f \equiv sf \bmod S\bar{I}_R$ where $s \in S$, $f \in F$, $r \in R$.

Since $S = \mathrm{Dr}_{x\in X}\, x(\mathbb{Z}F)$, we have $S\bar{I}_R = \mathrm{Dr}_{x \in X}\, x\bar{I}_R$, and

$$S/S\bar{I}_R \overset{G}{\simeq} \underset{x\in X}{\mathrm{Dr}}\; x(\mathbb{Z}F)/x\bar{I}_R \overset{G}{\simeq} \underset{x\in X}{\mathrm{Dr}}\; x(\mathbb{Z}(F/R)).$$

(ii) Clearly

$$ST = \underset{x\in X}{\mathrm{Dr}}\; x(\mathbb{Z}F)T = \underset{x\in X}{\mathrm{Dr}}\; xT = \underset{\substack{x\in X\\ y \in Y}}{\mathrm{Dr}}\; xy\mathbb{Z}F. \qquad \square$$

11.3.5 (The Gruenberg Resolution). *Let $R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} G$ be a presentation of a group G. Then there is a free right G-resolution of $\mathbb{Z}$*

$$\cdots \longrightarrow \bar{I}_R^n/\bar{I}_R^{n+1} \longrightarrow I_F\bar{I}_R^{n-1}/I_F\bar{I}_R^n \longrightarrow \bar{I}_R^{n-1}/\bar{I}_R^n \longrightarrow \cdots$$

$$\cdots \longrightarrow \bar{I}_R^2/\bar{I}_R^3 \longrightarrow I_F\bar{I}_R/I_F\bar{I}_R^2 \longrightarrow \bar{I}_R/\bar{I}_R^2 \longrightarrow I_F/I_F\bar{I}_R \longrightarrow \mathbb{Z}G \longrightarrow \mathbb{Z}.$$

The mappings here are as follows: $\mathbb{Z}G \to \mathbb{Z}$ is the augmentation, $I_F/I_F\bar{I}_R \to \mathbb{Z}G$ is induced by $\pi: F \to G$ and all other mappings are natural homomorphisms.

Proof. By 11.3.1 and 11.3.3 both I_F and $\bar{I}_R$ are free F-modules. Applying 11.3.4 we see that the modules $I_F\bar{I}_R^n/I_F\bar{I}_R^{n+1}$ and $\bar{I}_R^n/\bar{I}_R^{n+1}$ which appear in the complex are free G-modules. Now check exactness. The kernel of $\mathbb{Z}G \to \mathbb{Z}$ is I_G, which is also the image of $I_F/I_F\bar{I}_R \to \mathbb{Z}G$. The kernel of the latter map is $\bar{I}_R/I_F\bar{I}_R$ since $\bar{I}_R$ is the kernel of $\mathbb{Z}F \to \mathbb{Z}G$; the image of $\bar{I}_R/\bar{I}_R^2 \to I_F/I_F\bar{I}_R$ is also $\bar{I}_R/I_F\bar{I}_R$. And so on. $\square$

There is of course a corresponding *left* resolution in which the I_F appears on the *right* throughout. In the language of category theory 11.3.5 sets up a functor from presentations to resolutions—see Exercise 11.3.8.

The Standard Resolution

Let G be any group and let F be the free group on a set $\{x_g | 1 \neq g \in G\}$. Recall that the assignment $x_g \mapsto g$ gives rise to a presentation $R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} G$ called the standard presentation. We propose to examine the Gruenberg resolution that arises from this presentation: it is known as the *standard resolution.*

For convenience define x_1 to be 1; then the set $\{x_g | g \in G\}$ is a transversal to R in F. Since the nontrivial x_g are also free generators of F, it is clear that

this is a Schreier transversal in the sense of 6.1. It follows from 6.1.1 (and its proof) that R is freely generated by the elements

$$y_{g_1,g_2} = x_{g_1}x_{g_2}x_{g_1g_2}^{-1}, \qquad (1 \neq g_i \in G). \tag{14}$$

By 11.3.3 the $y_{g_1,g_2} - 1$ form a set of free generators for the free F-module $\bar{I}_R$. Define

$$(g_1, g_2) = x_{g_1g_2} - x_{g_1}x_{g_2} = (1 - y_{g_1,g_2})x_{g_1g_2} \tag{15}$$

where g_i belongs to G. Clearly $(g_1, g_2) \in \bar{I}_R$ and $(g_1, g_2) = 0$ if and only if g_1 or g_2 equals 1. Moreover (15) shows that *the nonzero* (g_1, g_2)*'s freely generate the* F*-module* $\bar{I}_R$.

Next we define for $n > 0$ the symbols

$$(g_1|g_2|\cdots|g_{2n}) = (g_1, g_2)(g_3, g_4)\cdots(g_{2n-1}, g_{2n}) + \bar{I}_R^{n+1}$$

and

$$(g_1|g_2|\cdots|g_{2n-1}) = (1 - x_{g_1})(g_2, g_3)(g_4, g_5)\cdots(g_{2n-2}, g_{2n-1}) + I_F\bar{I}_R^n.$$

These are elements of $P_{2n} = \bar{I}_R^n/\bar{I}_R^{n+1}$ and $P_{2n-1} = I_F\bar{I}_R^{n-1}/I_F I_R^n$ respectively. Observe that P_{2n} and P_{2n-1} together with $P_0 = \mathbb{Z}G$ are the terms of the Gruenberg resolution (11.3.5). We deduce from 11.3.4 that P_{2n} is freely generated as a G-module by the $(g_1|g_2|\cdots|g_{2n})$ and P_{2n-1} is freely generated as a G-module by the $(g_1|g_2|\cdots|g_{2n-1})$ where $1 \neq g_i \in G$. It is evident that $(g_1|g_2|\cdots|g_n) = 0$ if some g_i equals 1.

There is a useful formula describing the homomorphisms which appear in the standard resolution.

11.3.6. *The homomorphism* ∂_n: $P_n \to P_{n-1}$ *which occurs in the standard resolution is given by*

$$(g_1|\cdots|g_n)\partial_n = (g_2|\cdots|g_n) + \sum_{i=1}^{n-1}(-1)^i(g_1|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_n)$$
$$+ (-1)^n(g_1|\cdots|g_{n-1})g_n.$$

Proof. Consider the statement when $n = 1$. By definition $(g) = 1 - x_g + I_F\bar{I}_R$, so $(g)\partial_1 = 1 - g$, which agrees with the formula if we interpret $(g_r|\cdots|g_s)$ as 1 when $r > s$.

Next consider the case $n = 2$. Now ∂_2: $P_2 \to P_1$ maps $(g_1|g_2) = x_{g_1g_2} - x_{g_1}x_{g_2} + \bar{I}_R^2$ to $x_{g_1g_2} - x_{g_1}x_{g_2} + I_F\bar{I}_R$. The identity

$$x_{g_1g_2} - x_{g_1}x_{g_2} = (1 - x_{g_2}) - (1 - x_{g_1g_2}) + (1 - x_{g_1})x_{g_2}$$

shows that $(g_1|g_2)\partial_2 = (g_2) - (g_1g_2) + (g_1)g_2$, as predicted.

Now let $n = 3$. By definition ∂_3: $P_3 \to P_2$ maps

$$(g_1|g_2|g_3) = (1 - x_{g_1})(g_2, g_3) + I_F\bar{I}_R^2$$

to $(1 - x_{g_1})(g_2, g_3) + \bar{I}_R^2 = (1 - x_{g_1})(g_2|g_3)$. On the other hand, the value

predicted by the formula is

$$(g_2|g_3) - (g_1g_2|g_3) + (g_1|g_2g_3) - (g_1|g_2)g_3,$$

which is just

$$(x_{g_2g_3} - x_{g_2}x_{g_3}) - (x_{g_1g_2g_3} - x_{g_1g_2}x_{g_3}) + (x_{g_1g_2g_3} - x_{g_1}x_{g_2g_3}) - (x_{g_1g_2} - x_{g_1}x_{g_2})x_{g_3} + \bar{I}_R^2.$$

After cancellation this becomes $(1 - x_{g_1})(x_{g_2g_3} - x_{g_2}x_{g_3}) + \bar{I}_R^2$ or

$$(1 - x_{g_1})(g_2|g_3).$$

If $n > 3$, induction may be used to reduce to one of the cases already dealt with—for details see [b29]. □

Cocycles and Coboundaries

Let $\mathbf{P} \twoheadrightarrow \mathbb{Z}$ be the standard $\mathbb{Z}G$-resolution of $\mathbb{Z}$. Let us use this resolution to calculate $H^n(G, M)$ where M is any right G-module. One has to take the homology of the complex $\text{Hom}_G(\mathbf{P}, M)$; in this the homomorphisms are the

$$\delta^{n+1}: \text{Hom}_G(P_n, M) \longrightarrow \text{Hom}_G(P_{n+1}, M).$$

Now P_n is the free G-module on the set of all $(g_1|g_2|\cdots|g_n)$, $g_i \neq 1$. Thus a ψ in $\text{Hom}_G(P_n, M)$ is determined by its value at $(g_1|g_2|\cdots|g_n)$; conversely these values may be chosen arbitrarily in M to produce a ψ. Hence elements ψ of $\text{Hom}_G(P_n, M)$ correspond to functions $\varphi: \underbrace{G \times \cdots \times G}_{n} \to M$ such that $(g_1, \ldots, g_n)\varphi = 0$ if some g_i equals 1; the correspondence is given by

$$(g_1|\cdots|g_n)\psi = (g_1, \ldots, g_n)\varphi.$$

Such functions φ are called *n-cochains*. Note that $(g_1, \ldots, g_n)\varphi = 0$ if some $g_i = 1$.

The induced action of δ^{n+1} on n-cochains is easy to discover: $(\varphi)\delta^{n+1}$ corresponds to $(\psi)\delta^{n+1} = \partial_{n+1}\psi$. Using 11.3.6 we conclude that

$$\begin{aligned}(g_1, g_2, \ldots, g_{n+1})\varphi\delta^{n+1} &= (g_2, \ldots, g_{n+1})\varphi \\ &+ \sum_{i=1}^{n} (-1)^i (g_1, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots, g_{n+1})\varphi \\ &+ (-1)^{n+1}(g_1, \ldots, g_n)\varphi \cdot g_{n+1}. \qquad (16)\end{aligned}$$

If we write

$$Z^n(G, M) = \text{Ker } \delta^{n+1} \quad \text{and} \quad B^n(G, M) = \text{Im } \delta^n,$$

then

$$H^n(G, M) \simeq Z^n(G, M)/B^n(G, M). \qquad (17)$$

Elements of $Z^n(G, M)$ are called *n-cocycles* while those of $B^n(G, M)$ are *n-coboundaries.*

For example, suppose that $n = 1$. If $\varphi \in Z^1(G, M)$, then (16) shows that

$$0 = (g_2)\varphi - (g_1g_2)\varphi + (g_1)\varphi \cdot g_2$$

or $(g_1g_2)\varphi = ((g_1)\varphi)\cdot g_2 + (g_2)\varphi$, which is precisely the condition for φ to be a derivation from G to M.

Next if φ is a 0-cochain, which must be interpreted as a constant, that is, an element a of M, then $(g)\varphi\delta^1 = a(1 - g)$. Thus the 1-coboundary $(\varphi)\delta^1$ is just an inner derivation. We have therefore made the following identification:

$$H^1(G, M) = \mathrm{Der}(G, M)/\mathrm{Inn}(G, M). \tag{18}$$

If φ is a 2-cochain, the condition for φ to be a 2-cocycle is

$$(g_1, g_2g_3)\varphi + (g_2, g_3)\varphi = (g_1g_2, g_3)\varphi + (g_1, g_2)\varphi \cdot g_3$$

for all g_i in G. We recognize this as the factor set condition (6) encountered in 11.1.

11.3.7. *Let G be a finite group of order m. Suppose that M is any G-module. Then $m \cdot H^n(G, M) = 0$ for all $n > 0$.*

Proof. Let $\varphi: \underbrace{G \times \cdots \times G}_{n} \to M$ be any n-cochain. There is a corresponding $(n - 1)$-cochain ψ given by

$$(g_2, \ldots, g_n)\psi = \sum_{x \in G} (x, g_2, \ldots, g_n)\varphi.$$

Sum the formula (16) over all $g_1 = x$ in G to get

$$\begin{aligned}\sum_{x \in G} (x, g_2, \ldots, g_{n+1})\varphi\delta^{n+1} = m((g_2, \ldots, g_{n+1})\varphi)& \\ + \sum_{i=2}^{n} (-1)^i(g_2, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots, g_{n+1})\psi& \\ - (g_3, \ldots, g_{n+1})\psi + (-1)^{n+1}(g_2, \ldots, g_n)\psi \cdot g_{n+1}.&\end{aligned}$$

If $\varphi \in Z^n(G, M)$, this becomes $m\varphi = \psi\delta^n$, so that $m\varphi \in B^n(G, M)$ and

$$m \cdot H^n(G, M) = 0. \qquad \square$$

This has the following useful corollary.

11.3.8. *Let G be a finite group of order m. Suppose that M is a G-module which is uniquely divisible by m. Then $H^n(G, M) = 0$ for all $n > 0$.*

Proof. Let $\varphi \in Z^n(G, M)$: then $m\varphi = \psi\delta^n$ for some $(n - 1)$-cochain ψ by 11.3.7. Since M is uniquely divisible by m, it is meaningful to define $\bar{\psi}$ to be $(1/m)\psi$. Then $\bar{\psi}$ is an $(n - 1)$-cochain and $\varphi = \bar{\psi}\delta^n \in B^n(G, M)$. Thus $H^n(G, M) = 0$. $\square$

The corresponding results for homology are also true but require a different proof (see Exercise 11.3.10).

EXERCISES 11.3

*1. For any group G show that I_G is a free abelian group on the set $G - 1 = \{g - 1 | 1 \neq g \in G\}$.

2. Let $G = \langle g \rangle$ be an infinite cyclic group. Using the presentation $1 \rightarrowtail G \twoheadrightarrow G$ write down the left and right Gruenberg resolutions for G. If M is a G-module, show that $H^0(G, M) \simeq M^G \simeq H_1(G, M)$ and $H^1(G, M) \simeq M_G \simeq H_0(G, M)$ where $M^G = \{a \in M | ag = a\}$ and $M_G = M/M(g - 1)$.

3. If F is a free group and M is an F-module, use the Gruenberg resolution to calculate $H^0(F, M)$ and $H^1(F, M)$.

4. The same question for $H_0(F, M)$ and $H_1(F, M)$.

5. Let $G = \langle g \rangle$ be a cyclic group of finite order m. If F is an infinite cyclic group, show that the presentation $F^m \rightarrowtail F \twoheadrightarrow G$ determines a resolution

$$\cdots \longrightarrow \mathbb{Z}G \xrightarrow{\beta} \mathbb{Z}G \xrightarrow{\alpha} \mathbb{Z}G \xrightarrow{\beta} \mathbb{Z}G \xrightarrow{\alpha} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

where α and β are multiplication by $g - 1$ and $1 + g + \cdots + g^{m-1}$, respectively.

6. Use the previous exercise to calculate the (co)homology of a cyclic group G of order m. If M is any G-module, then for $n > 0$

$$H^{2n-1}(G, M) \simeq \operatorname{Ker} \beta/\operatorname{Im} \alpha \qquad \text{and} \qquad H^{2n}(G, M) \simeq \operatorname{Ker} \alpha/\operatorname{Im} \beta.$$

Also

$$H_n(G, M) \simeq H^{n+1}(G, M).$$

7. Let G be a finite cyclic group and let M be a finite G-module. Assume that $H^i(G, M) = 0$ for some fixed $i > 0$. Prove that $H^n(G, M) = 0$ for all $n > 0$. [Use Exercise 11.3.6.]

8. (a) Let $R_i \rightarrowtail F_i \twoheadrightarrow G$, $i = 1, 2$, be two presentations of a group G. Prove that there is a morphism $(\alpha, \beta, 1)$ from $R_1 \rightarrowtail F_1 \twoheadrightarrow G$ to $R_2 \rightarrowtail F_2 \twoheadrightarrow G$.
   (b) Prove that any such morphism of presentations of G determines a morphism of the correspondence Gruenberg resolutions.
   (c) The association of a Gruenberg resolution with a presentation determines a functor from the category of presentations of G to the category of free G-resolutions of $\mathbb{Z}$.

9. Let G be the union of a countable chain of groups $G_1 \leq G_2 \leq \cdots$. Let M be a G-module such that $H^n(G_i, M) = 0 = H^{n+1}(G_i, M)$ for all i and for some fixed n. Prove that $H^{n+1}(G, M) = 0$.

10. Let G be a finite group of order m and let M be any right G-module. By adopting the following procedure (due to R. Strebel) prove that $m \cdot H_n(G, M) = 0$ if $n > 0$.
    (a) Let $\mathbf{F}$ be a free left $\mathbb{Z}G$-resolution of $\mathbb{Z}$. Define morphisms of complexes $\alpha\colon M \otimes_{\mathbb{Z}G} \mathbf{F} \to M \otimes_{\mathbb{Z}} \mathbf{F}$ and $\beta\colon M \otimes_{\mathbb{Z}} \mathbf{F} \to M \otimes_{\mathbb{Z}G} \mathbf{F}$ by $(a \otimes b)\alpha_i = \sum_{g \in G} ag \otimes g^{-1}b$ and $(a \otimes b)\beta_i = a \otimes b$ where $a \in M$ and $b \in F_i$.

(b) Show that $\alpha\beta$ induces homomorphisms $H_n(M \otimes_{\mathbb{Z}G} \mathbf{F}) \to H_n(M \otimes_{\mathbb{Z}G} \mathbf{F})$ which are simply multiplication by m on each module.
(c) Prove that $M \otimes_{\mathbb{Z}} \mathbf{F}$ is exact, noting that if $A \rightarrowtail B \twoheadrightarrow C$ is an exact sequence of *free* abelian groups, then $M \otimes A \rightarrowtail M \otimes B \twoheadrightarrow M \otimes C$ is an exact sequence (with the obvious maps).
(d) Deduce from (b) and (c) that $m \cdot H_n(G, M) = 0$.

11.4. Group-Theoretic Interpretations of the (Co)homology Groups

The group-theoretic significance of the homology and cohomology groups in low dimensions will now be discussed.

The Groups $H_0(G, M)$ and $H^0(G, M)$

To compute $H_0(G, M)$ we tensor the *left* Gruenberg resolution by M, obtaining

$$\cdots \longrightarrow M \otimes_{\mathbb{Z}G} (I_F/\bar{I}_R I_F) \longrightarrow M \otimes_{\mathbb{Z}G} \mathbb{Z}G \longrightarrow 0.$$

Now $M \otimes_{\mathbb{Z}G} \mathbb{Z}G \overset{G}{\simeq} M$ via the mapping $a \otimes g \mapsto ag$. Therefore by definition of the homology groups $H_0(G, M)$ is isomorphic with M/MI_G, *the largest G-trivial quotient of* M; this is usually written M_G.

In a similar manner it may be shown that

$$H^0(G, M) \simeq \{a \in M \mid ag = a, \forall g \in G\},$$

the set of G-fixed points of M, which is often written M^G (confusion with normal closures being unlikely). Thus we have

11.4.1. *If G is a group and M a right G-module, then*

$$H_0(G, M) \simeq M_G \qquad \text{and} \qquad H^0(G, M) \simeq M^G.$$

The Group $H_1(G, M)$

11.4.2. *If G is a group and M a right G-module, then $H_1(G, M)$ is isomorphic with the kernel of the homomorphism $M \otimes_{\mathbb{Z}G} I_G \to M$ in which*

$$a \otimes (g - 1) \mapsto a(g - 1).$$

This follows at once when 11.2.7 is applied to the Gruenberg resolution. There is a neat formula for $H_1(G, M)$ when G operates trivially on M. In order to derive this we take note of a result which has some interest in itself.

11.4.3. *If G is any group, then $I_G/I_G^2 \simeq G_{ab}$.*

Proof. Since I_G is free on $\{g - 1 | 1 \neq g \in G\}$ as an abelian group, the mapping $x - 1 \mapsto xG'$ determines a homomorphism $I_G \to G_{ab}$. Now the identity $(x - 1)(y - 1) = (xy - 1) - (x - 1) - (y - 1)$ implies that I_G^2 is mapped to 0. Hence there is an induced homomorphism $\varphi: I_G/I_G^2 \to G_{ab}$ such that $((x - 1) + I_G^2)\varphi = xG'$. On the other hand, $x \mapsto (x - 1) + I_G^2$ is a homomorphism from G to I_G/I_G^2 by the same identity. Therefore it induces a homomorphism $G_{ab} \to I_G I_G^2$ which is clearly inverse to φ. □

11.4.4. *If M is a trivial right G-module, then $H_1(G, M) \simeq M \otimes G_{ab}$.*

Proof. By 11.4.2 we have $H_1(G, M) \simeq M \otimes_{\mathbb{Z}G} I_G$. It is seen that the assignment $a \otimes (x - 1) \mapsto a \otimes ((x - 1) + I_G^2)$ yields an isomorhism

$$M \otimes_{\mathbb{Z}G} I_G \xrightarrow{\simeq} M \otimes_{\mathbb{Z}} (I_G/I_G^2).$$

The result now follows from 11.4.3. □

The Group $H^1(G, M)$

An interpretation of $H^1(G, M)$ as the quotient group $\mathrm{Der}(G, M)/\mathrm{Inn}(G, M)$ has already been mentioned during our discussion of the standard resolution. Another approach to this important result will now be given based on a lemma for which we shall find other uses.

11.4.5. *If G is a group and M a G-module, then* $\mathrm{Der}(G, M) \simeq \mathrm{Hom}_G(I_G, M)$.

Proof. If $\delta \in \mathrm{Der}(G, M)$, we may define a homomorphism $\delta^*: I_G \to M$ by $(g - 1)\delta^* = g\delta$, keeping in mind that I_G is free as an abelian group on the set $\{g - 1 | 1 \neq g \in G\}$. For g_1, g_2 in G we have $(g_1 - 1)g_2 = (g_1 g_2 - 1) - (g_2 - 1)$, which implies that

$$((g_1 - 1)g_2)\delta^* = (g_1 g_2)\delta - g_2\delta = (g_1\delta)g_2 = ((g_1 - 1)\delta^*)g_2.$$

Hence $\delta^* \in \mathrm{Hom}_G(I_G, M)$. Conversely, if $\theta \in \mathrm{Hom}_G(I_G, M)$, define $g\theta^* = (g - 1)\theta$; a similar calculation shows that $\theta^* \in \mathrm{Der}(G, M)$. Of course $\delta \mapsto \delta^*$ and $\theta \mapsto \theta^*$ are inverse mappings. It is equally clear that $\delta \mapsto \delta^*$ is a homomorphism of abelian groups. Thus $\delta \mapsto \delta^*$ is an isomorphism. □

11.4.6. *If G is a group and M a G-module, then*

$$H^1(G, M) \simeq \mathrm{Der}(G, M)/\mathrm{Inn}(G, M).$$

Proof. Applying 11.2.7 to the Gruenberg resolution we obtain the exact sequence

$$\mathrm{Hom}_G(\mathbb{Z}G, M) \longrightarrow \mathrm{Hom}_G(I_G, M) \longrightarrow H^1(G, M) \longrightarrow 0. \qquad (19)$$

According to 11.4.5 the middle group is isomorphic with $\mathrm{Der}(G, M)$. Note that $\varphi \in \mathrm{Hom}_G(\mathbb{Z}G, M)$ is completely determined by $(1)\varphi = a$ in M; for then $(g)\varphi = ag$. The image of φ in $\mathrm{Hom}_G(I_G, M)$ is the restriction of φ to I_G, which corresponds to the derivation $g \mapsto (g - 1)\varphi = a(g - 1)$, that is, to an inner derivation. Thus $\mathrm{Inn}(G, M)$ corresponds to the image of the left hand mapping in (19). It follows that the sequence

$$0 \longrightarrow \mathrm{Inn}(G, M) \longrightarrow \mathrm{Der}(G, M) \longrightarrow H^1(G, M) \longrightarrow 0 \qquad (20)$$

is exact. The required isomorphism is a consequence of (20). □

Combining 11.4.6 with 11.1.3 we obtain the next result.

11.4.7. *Let G be a group and M a G-module. All complements of M in the associated semidirect product $G \ltimes M$ are conjugate if and only if $H^1(G, M) = 0$.*

MacLane's Theorem

We come now to the connection between the second cohomology group and extension theory. First, however, a simple observation must be made.

11.4.8. *Let $R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} G$ be a presentation of a group G. Then the mapping $rR' \mapsto (r - 1) + I_F\bar{I}_R$ is a G-isomorphism from R_{ab} to $\bar{I}_R/I_F\bar{I}_R$.*

Proof. Of course R_{ab} is a G-module via conjugation in F: thus $(rR')^{f^\pi} = (f^{-1}rf)R'$ where $r \in R$ and $f \in F$. Let $T = \bar{I}_R/I_F\bar{I}_R$ and consider the mapping $r \mapsto (r - 1) + I_F\bar{I}_R$ from R to T. Now if r_1, r_2 are elements of R,

$$\begin{aligned} r_1r_2 - 1 &= (r_1 - 1) + (r_2 - 1) + (r_1 - 1)(r_2 - 1) \\ &\equiv (r_1 - 1) + (r_2 - 1) \mod I_F\bar{I}_R. \end{aligned}$$

This shows that $r \mapsto (r - 1) + I_F\bar{I}_R$ is a homomorphism of groups. Since T is abelian, there is an induced homomorphism $\theta\colon R_{ab} \to T$.

Let us check that θ is a G-homomorphism;

$$\begin{aligned} ((rR')^{f^\pi})^\theta &= (f^{-1}rfR')^\theta = (f^{-1}rf - 1) + I_F\bar{I}_R \\ &= f^{-1}(r - 1)f + I_F\bar{I}_R \\ &= (r - 1)f + I_F\bar{I}_R = ((rR')^\theta)f^\pi. \end{aligned}$$

Finally, in order to show that θ is an isomorphism we shall produce an inverse. Let R be free on X. By 11.3.3 for left R-modules we have $\bar{I}_R = \mathrm{Dr}_{x \in X}\, \mathbb{Z}F(x - 1)$, so that $T = \bar{I}_R/I_F\bar{I}_R$ equals $\mathrm{Dr}_{x \in X}(\mathbb{Z}F)(x - 1)/I_F(x - 1)$ and hence is isomorphic with $\mathrm{Dr}_{x \in X}(\mathbb{Z}F/I_F)(x - 1)$. Since $\mathbb{Z}F/I_F \simeq \mathbb{Z}$, we conclude that T is the free abelian group on the set of all

$(x - 1) + I_F\bar{I}_R$, $x \in X$. Hence there is a group homomorphism $\psi: T \to R_{ab}$ such that $((x - 1) + I_F\bar{I}_R)\psi = xR'$. Obviously ψ is the inverse of θ. □

11.4.9 (MacLane). *Let $R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} G$ be a presentation of a group G. Let M be any right G-module. Then there is an exact sequence*

$$H^1(F, M) \longrightarrow \mathrm{Hom}_G(R_{ab}, M) \longrightarrow H^2(G, M) \longrightarrow 0.$$

Proof. Here M is an F-module via π, so that $af = af^\pi$ where $a \in M$, $f \in F$. Apply 11.2.7 using the Gruenberg resolution associated with the given presentation. There results an exact sequence

$$\mathrm{Hom}_G(I_F/I_F\bar{I}_R, M) \longrightarrow \mathrm{Hom}_G(\bar{I}_R/I_F\bar{I}_R, M) \longrightarrow H^2(G, M) \longrightarrow 0. \quad (21)$$

Recall that the left-hand map is induced by the inclusion $\bar{I}_R/I_F\bar{I}_R \to I_F/I_F\bar{I}_R$. By 11.4.8 we have $\bar{I}_R/I_F\bar{I}_R \simeq R_{ab}$, so the middle group in the exact sequence is isomorphic with $\mathrm{Hom}_G(R_{ab}, M)$.

We claim that

$$\mathrm{Hom}_G(I_F/I_F\bar{I}_R, M) \simeq \mathrm{Hom}_F(I_F, M).$$

To see this let $\alpha: I_F \to M$ be an F-homomorphism. Then α maps $I_F\bar{I}_R$ to 0; for, on the basis of the trivial action of R on M, we have $((f - 1)(r - 1))\alpha = (f - 1)\alpha \cdot (r - 1) = 0$. Hence α induces a homomorphism $\bar{\alpha}: I_F/I_F\bar{I}_R \to M$. It is clear that $\alpha \mapsto \bar{\alpha}$ is an isomorphism, so the assertion is true.

Next $\mathrm{Der}(F, M) \simeq \mathrm{Hom}_F(I_F, M)$ by 11.4.5. Hence (21) becomes

$$\mathrm{Der}(F, M) \longrightarrow \mathrm{Hom}_G(R_{ab}, M) \longrightarrow H^2(G, M) \longrightarrow 0. \quad (22)$$

We have, of course, to keep track of the left-hand mapping; it is the obvious one $\delta \mapsto \delta'$ where δ' is induced in R_{ab} by δ. If δ is inner, there is an a in M such that $(rR')^{\delta'} = a(-r + 1) = 0$ for all r in R; this is because R operates trivially on M. Consequently $\mathrm{Inn}(F, M)$ maps to 0. The result now follows from 11.4.6. □

The Second Cohomology Group and Extensions

Let G and N be groups and let $\chi: G \to \mathrm{Out}\, N$ be a coupling of G to N. Let us assume that there is at least one extension that realizes χ. Recall from 11.1.8 that there is a bijection between the set of equivalence classes of extensions of N by G with coupling χ and the cokernel of $\mathrm{Der}(F, C) \to \mathrm{Hom}_F(R, C)$; here C is the center of N. Now $\mathrm{Hom}(R, C) \simeq \mathrm{Hom}(R_{ab}, C)$ and R acts trivially on R_{ab}; thus $\mathrm{Hom}_F(R, C) \simeq \mathrm{Hom}_G(R_{ab}, C)$. We have to deal with the cokernel of the obvious mapping $\mathrm{Der}(F, C) \to \mathrm{Hom}_G(R_{ab}, C)$; by (22) this is isomorphic with $H^2(G, C)$.

We have proved a fundamental theorem.

11.4.10. *Let G and N be groups and let χ be a coupling of G to N. Assume that χ is realized by at least one extension of N by G. Then there is a bijection between equivalence classes of extensions of N by G with coupling χ and elements of the group $H^2(G, C)$ where C is the center of N regarded as a G-module via χ.*

When N is abelian, this reduces 11.1.4, which was proved by using factor sets.

Extensions with Abelian Kernel

It has been pointed out that when N is abelian, every coupling of G to N is realized by some extension, for example the split extension, which corresponds to 0 in $H^2(G, N)$.

It is worthwhile being more explicit in this important case.

11.4.11. *Let G be a group, A a G-module and $R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} G$ any presentation of G. Let $\Delta \in H^2(G, A)$ and suppose that φ is a preimage of Δ under the mapping $\mathrm{Hom}_G(R_{\mathrm{ab}}, A) \to H^2(G, A)$ of MacLane's Theorem. Then*

$$A \rightarrowtail (F \ltimes A)/R^{\varphi'} \twoheadrightarrow G$$

is an extension which induces the prescribed G-module structure in A and whose equivalence class corresponds to Δ.

Here A is regarded as an F-module via $\pi: F \to G$. To comprehend 11.4.11 it is necessary to look back at the proof of 11.1.8. We take R to be the fixed element of $\mathscr{M}$ in that proof, which is possible since A is abelian. The equivalence class of $R^{\varphi'}$ corresponds to $\varphi + I$ where I is the image of $\mathrm{Der}(F, C)$; this $\varphi + I$ corresponds to Δ.

The next result is essentially the abelian case of the Schur–Zassenhaus Theorem (9.1.2).

11.4.12. *Let G be a finite group of order m. Suppose that A is a G-module such that each element of A is uniquely divisible by m. Then every extension of A by G splits and all complements of A are conjugate.*

This follows directly from 11.3.8, 11.4.7, and 11.4.10.

Central Extensions

An extension $C \overset{\mu}{\rightarrowtail} E \twoheadrightarrow G$ is called *central* if $\mathrm{Im}\,\mu$ is contained in the centre of E. In this case G operates trivially on C, so that C is a trivial G-module.

Such extensions are frequently encountered; for example every nilpotent group can be constructed from abelian groups by means of a sequence of central extensions.

Suppose that C is a trivial G-module and let $R \rightarrowtail F \twoheadrightarrow G$ be a presentation of G. Let us interpret MacLane's Theorem in this case. Of course F, like G, operates trivially on C, and

$$\mathrm{Der}(F, C) = \mathrm{Hom}(F, C) \simeq \mathrm{Hom}(F_{ab}, C).$$

Also

$$\mathrm{Hom}_G(R_{ab}, C) \simeq \mathrm{Hom}(R/[F, R], C)$$

because $[F, R]/R'$ must map to 1 under any G-homomorphism from R_{ab} to C. As a consequence of these remarks MacLane's Theorem takes the following form.

11.4.13. *If C is a trivial G-module and $R \rightarrowtail F \twoheadrightarrow G$ is a presentation of the group G, there is an exact sequence*

$$\mathrm{Hom}(F_{ab}, C) \longrightarrow \mathrm{Hom}(R/[R, F], C) \longrightarrow H^2(G, C) \longrightarrow 0.$$

Thus each central extension of C by G arises from a homomorphism $\varphi: R/[R, F] \to C$.

Abelian Extensions

A central extension of one abelian group by another is usually not abelian —consider for example the quaternion group Q_8. Suppose that G is an abelian group and C a trivial G-module. Call the extension $C \rightarrowtail E \twoheadrightarrow G$ *abelian* if E is an abelian group. There are, of course, always abelian extensions, for example the direct product extension, $C \rightarrowtail C \times G \twoheadrightarrow G$.

The equivalence classes of abelian extensions correspond to a certain subset

$$\mathrm{Ext}(G, A)$$

of $H^2(G, A)$.

Let us use 11.4.11 to determine which central extensions are abelian; in the sequel G is an abelian group. As usual choose a presentation $R \rightarrowtail F \twoheadrightarrow G$ here of course $F' \leq R$. By 11.4.11 a central extension of C by G is equivalent to one of the form

$$C \rightarrowtail (F \times C)/R^{\varphi'} \twoheadrightarrow G$$

where $\varphi \in \mathrm{Hom}_G(R_{ab}, C)$. This extension is abelian if and only if $F' \leq R^{\varphi'}$. Let $f \in F'$ and $r \in R$; if $f = r^{\varphi'} = rr^{\varphi}$, we observe that $r^{\varphi} = r^{-1}f \in F \cap C = 1$; thus $f = r$ and $f^{\varphi} = r^{\varphi} = 1$. Hence φ maps F' to 1. Conversely, if $\varphi \in \mathrm{Hom}_G(R_{ab}, C)$ maps F' to 1, then $f^{\varphi'} = ff^{\varphi} = f$ if $f \in F'$. Thus $F' \leq R^{\varphi'}$. It follows that the abelian extensions are determined by elements of $\mathrm{Hom}(R/F', C)$. *Thus* $\mathrm{Ext}(G, C)$ *is a subgroup of* $H^2(G, C)$.

11.4.14. *Let G and C be abelian groups. Suppose that $R \rightarrowtail F \twoheadrightarrow G$ is a presentation of G. Then there is an exact sequence of abelian groups*

$$\mathrm{Hom}(F_{\mathrm{ab}}, C) \longrightarrow \mathrm{Hom}(R/F', C) \longrightarrow \mathrm{Ext}(G, C) \longrightarrow 0.$$

This follows on combining the preceding remarks with 11.4.13.

The Schur Multiplicator

Let G be any group and let $\mathbb{Z}$ be regarded as a trivial G-module. For brevity it is customary to write

$$H_n G = H_n(G, \mathbb{Z}),$$

the *integral homology group* of degree n. For example $H_1 G \simeq \mathbb{Z} \otimes G_{\mathrm{ab}} \simeq G_{\mathrm{ab}}$ by 11.4.4. The group

$$M(G) = H_2 G$$

is known as the *Schur multiplicator* of G. It plays a prominent role in Schur's theory of projective representations. We shall see that it is also relevant to the theory of central extensions.

There is an interesting formula for $M(G)$.

11.4.15 (Hopf's Formula). *If $R \rightarrowtail F \twoheadrightarrow G$ is a presentation of a group G, then*

$$M(G) \simeq F' \cap R/[F, R].$$

In particular this factor does not depend on the presentation.

Proof. Apply 11.2.7 to the *left* Gruenberg resolution. There results

$$M(G) \simeq \mathrm{Ker}(\mathbb{Z} \otimes_{\mathbb{Z}G} (\bar{I}_R/\bar{I}_R I_F) \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}G} (I_F/\bar{I}_R I_F)).$$

Now $\bar{I}_R/\bar{I}_R I_F$ is isomorphic as a *left* G-module with R_{ab} by the left version of 11.4.8—here R_{ab} is to be regarded as a *left* G-module via the action ${}^{fR}(rR') = (frf^{-1})R'$. Also $\mathbb{Z} \otimes_{\mathbb{Z}G} R_{\mathrm{ab}} \simeq R/[F, R]$ via $n \otimes rR' \mapsto r^n[F, R]$. In addition $\mathbb{Z} \otimes_{\mathbb{Z}G} (I_F/\bar{I}_R I_F) \simeq I_F/I_F^2$ for a similar reason. By 11.4.3 we have $I_F/I_F^2 \simeq F_{\mathrm{ab}}$. It follows that

$$M(G) \simeq \mathrm{Ker}(R/[F, R] \longrightarrow F_{\mathrm{ab}}),$$

the map being the obvious one, $r[F, R] \mapsto rF'$. The kernel is clearly $F' \cap R/[F, R]$. □

In the case of abelian groups there is a simpler formula for the Schur multiplicator. If G is an abelian group, define

$$G \wedge G = (G \otimes G)/D$$

where $D = \langle g \otimes g | g \in G \rangle$. This is called the *exterior square* of G. If $g_1 \wedge g_2$ denotes $g_1 \otimes g_2 + D$, then $(g_1 + g_2) \wedge (g_1 + g_2) = 0$, which shows that $g_1 \wedge g_2 = -(g_2 \wedge g_1)$. Thus $G \wedge G$ may be regarded as a skew-symmetric tensor product.

11.4.16. *If G is an abelian group, then $M(G) \simeq G \wedge G$.*

Proof. Let $R \rightarrowtail F \twoheadrightarrow G$ be a presentation of G. Since G is abelian, $F' \leq R$ and $M(G) \simeq F'/[F, R]$ by Hopf's formula. The mapping $(f_1R, f_2R) \mapsto [f_1, f_2][F, R]$, $(f_i \in F)$, is well-defined and bilinear. Consequently there is an induced homomorphism $(F/R) \otimes (F/R) \to F'[F, R]$ by the fundamental mapping property of the tensor product. What is more, $fR \otimes fR$ maps to 1, so there is induced a homomorphism θ: $(F/R) \wedge (F/R) \to F'/[F, R]$ in which $f_1R \wedge f_2R$ is sent to $[f_1, f_2][F, R]$.

To construct an inverse of θ choose a set of free generators $\{x_1, x_2, \dots\}$ for F. By Exercise 6.1.14 the group $F'/\gamma_3 F$ is free abelian with free generators the $[x_i, x_j]\gamma_3 F$, where $i < j$. Hence there is a homomorphism ϕ_0: $F'/\gamma_3 F \to (F/R) \wedge (F/R)$ sending $[x_i, x_j]\gamma_3 F$ to $x_iR \wedge x_jR$. Now for any $f_1, f_2 \in F$ we see from bilinearity of the commutator that $([f_1, f_2]\gamma_3 F)^{\phi_0} = f_1R \wedge f_2R$. Hence ϕ_0 maps $[F, R]/\gamma_3 F$ to 0, and so there is an induced homomorphism ϕ: $F'/[F, R] \to (F/R) \wedge (F/R)$. Clearly θ and ϕ are inverse functions. □

For example, if G is an elementary abelian p-group of rank r, then $M(G) \simeq G \wedge G$ is an elementary abelian p-group of rank $\binom{r}{2}$ (Exercise 11.4.9).

Hopf's formula can be used to associate an exact sequence of homology groups with any extension. This will be applied in Chapter 14 to the study of one-relator groups.

11.4.17 (The Five-Term Homology Sequence). *Corresponding to any group extension $N \rightarrowtail E \overset{\varepsilon}{\twoheadrightarrow} G$ there is an exact sequence*

$$M(E) \longrightarrow M(G) \longrightarrow N/[E, N] \longrightarrow E_{\mathrm{ab}} \longrightarrow G_{\mathrm{ab}} \longrightarrow 1.$$

This sequence is natural in the following sense. Given a morphism (α, β, γ) from $N \rightarrowtail E \twoheadrightarrow G$ to $\bar{N} \rightarrowtail \bar{E} \twoheadrightarrow \bar{G}$ there are induced homomorphisms α_*, β_*, γ_*, making the diagram

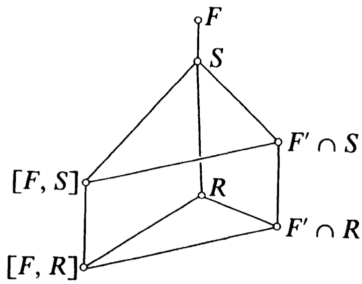
$$\begin{array}{ccccccccccc}
M(E) & \longrightarrow & M(G) & \longrightarrow & N/[E, N]) & \longrightarrow & E_{\mathrm{ab}} & \longrightarrow & G_{\mathrm{ab}} & \longrightarrow & 1 \\
\downarrow{\scriptstyle \beta_*} & & \downarrow{\scriptstyle \gamma_*} & & \downarrow{\scriptstyle \alpha_*} & & \downarrow{\scriptstyle \beta_*} & & \downarrow{\scriptstyle \gamma_*} & & \\
M(\bar{E}) & \longrightarrow & M(\bar{G}) & \longrightarrow & \bar{N}/(\bar{E}, \bar{N}]) & \longrightarrow & \bar{E}_{\mathrm{ab}} & \longrightarrow & \bar{G}_{\mathrm{ab}} & \longrightarrow & 1
\end{array}$$

commutative.

Proof. Here of course we can take N to be a subgroup of E as a matter of convenience.

The mappings $N/[E, N] \to E_{ab}$ and $E_{ab} \to G_{ab}$ are the obvious ones, $x[E, N] \mapsto xE'$ and $xE' \mapsto x^{\varepsilon}G'$ respectively. Exactness at E_{ab} and G_{ab} is easily checked. It remains to construct the other two mappings and check exactness at $M(G)$ and $N/[E, N]$.

Let $R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} E$ be some presentation of E. Then $\pi\varepsilon: F \to G$ is a presentation of G; let $\operatorname{Ker} \pi\varepsilon = S$. By Hopf's formula $M(E) \simeq F' \cap R/[F, R]$ and $M(G) \simeq F' \cap S/[F, S]$. Now S is the preimage of N under π, so in fact $R \leq S$ and $S/R \simeq N$. The relevant subgroups are situated as follows:



Define $M(G) \to N/[E, N]$ by means of $x[F, S] \mapsto x^{\pi}[E, N]$ and $M(G) \simeq F' \cap S/[F, S]$. The image of this mapping is clearly $E' \cap N/[E, N]$, which is the kernel of $N/[E, N] \to E_{ab}$. This establishes exactness at $N/[E, N]$.

Finally, define $M(E) \to M(G)$ by means the natural homomorphism from $F' \cap R/[F, R]$ to $(F' \cap R)[F, S]/[F, S]$, together with Hopf's formula. The kernel of $M(G) \to N/[E, N]$ corresponds to $(F' \cap R)[F, S]/[F, S]$, so the sequence is also exact at $M(G)$.

We shall not take the space to establish naturality (see however Exercise 11.4.16). □

To conclude this discussion of the Schur multiplicator we mention an important result that illustrates the relationship between the multiplicator and the theory of central extensions. A proof is sketched in Exercise 11.4.5.

11.4.18 (Universal Coefficients Theorem). *If G is a group and M a trivial G-module, there is an exact sequence*

$$\operatorname{Ext}(G_{ab}, M) \rightarrowtail H^2(G, M) \twoheadrightarrow \operatorname{Hom}(M(G), M).$$

The mapping on the right shows that every central extension of M by G gives rise to a homomorphism from $M(G)$ to M.

An important special case occurs when G is perfect; for then $\operatorname{Ext}(G_{ab}, M) = 0$ and

$$H^2(G, M) \simeq \operatorname{Hom}(M(G), M),$$

so equivalence classes of central extensions of M and G stand in one-to-one correspondence with homomorphisms from $M(G)$ to M.

The Third Cohomology Group and Obstructions

Finally we shall address the third major problem of extension theory. Given groups N and G together with a coupling $\chi: G \to \operatorname{Out} N$, when does there exist an extension of N by G which realizes the coupling χ?

We shall write C for the centre of N, keeping in mind that χ prescribes a G-module structure for C.

Choose any presentation $R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} G$ of G. Just as in 11.1—see equation (7)—we can find homomorphisms ξ and η which make the diagram

$$\begin{array}{ccccc} R & \rightarrowtail & F & \overset{\pi}{\twoheadrightarrow} & G \\ {\scriptstyle\eta}\downarrow & & {\scriptstyle\xi}\downarrow & & {\scriptstyle\chi}\downarrow \\ N & \overset{\tau}{\longrightarrow} & \operatorname{Aut} N & \overset{\nu}{\twoheadrightarrow} & \operatorname{Out} N \end{array} \tag{23}$$

commutative: here τ is the conjugation homomorphism and ν the natural homomorphism. If $r \in R$ and $f \in F$, the element $(r^\eta)^{-1}((r^{f^{-1}})^\eta)^{f^\xi}$ surely belongs to N. Let us apply the function τ to this element, observing that $\eta\tau = \xi$ by commutativity of the diagram, and that $(x^\alpha)^\tau = (x^\tau)^\alpha$ if $\alpha \in \operatorname{Aut} N$. We obtain

$$(r^\xi)^{-1}((r^{f^{-1}})^\xi)^{f^\xi} = (r^\xi)^{-1} r^\xi = 1,$$

so that the element

$$f * r = (r^\eta)^{-1}((r^{f^{-1}})^\eta)^{f^\xi} \tag{24}$$

belongs to $\operatorname{Ker} \tau$, that is to C, the center of N.

Using the definition (24) it is completely straightforward to verify the formulae

$$f * (r_1 r_2) = (f * r_1)(f * r_2) \tag{25}$$

and

$$(f_1 f_2) * r = (f_2 * r)(f_1 * r^{f_2^{-1}})^{f_2^\xi}. \tag{26}$$

Let us now consider the Gruenberg resolution that is associated with the chosen presentation of G. Suppose that F is free on a set X and R is free on a set Y. Since $I_F \bar{I}_R / I_F \bar{I}_R^2$ is free as a G-module on the set of all $(1 - x)(1 - y) + I_F \bar{I}_R^2$, $(x \in X, y \in Y)$, by 11.3.3 and 11.3.4, the assignment

$$(1 - x)(1 - y) + I_F \bar{I}_R^2 \longmapsto x * y$$

determines a G-homomorphism

$$\psi: I_F \bar{I}_R / I_F \bar{I}_R^2 \longrightarrow C.$$

Next one observes that $((1 - x)(1 - r) + I_F \bar{I}_R^2)\psi = x * r$, $(x \in X, r \in R)$. This

follows by (25) and induction on the length of r, together with the equation

$$(1 - x)(1 - r_1 r_2) = (1 - x)((1 - r_1) + (1 - r_2) - (1 - r_1)(1 - r_2)).$$

In a similar way one can prove that

$$((1 - f)(1 - r) + I_F \bar{I}_R^2)\psi = f * r \tag{27}$$

for all f in F and r in R; this may be accomplished by using induction on the length of f, equation (26) and also the equation

$$(1 - f_1 f_2)(1 - r) = (1 - f_2)(1 - r) + (1 - f_1)(1 - r^{f_2^{-1}})f_2.$$

If $r_i \in R$, the definition (24) tells us that $r_1 * r_2 = (r_2^\eta)^{-1}((r_2^{r_1^{-1}})^\eta)^{r_1^\eta} = (r_2^\eta)^{-1} r_2^\eta = 1$. Equation (27) now shows that ψ maps $\bar{I}_R^2 / I_F \bar{I}_R^2$ to 1. Consequently ψ induces a homomorphism φ from $I_F \bar{I}_R / \bar{I}_R^2$ to C. We call this homomorphism

$$\varphi \in \mathrm{Hom}_G(I_F \bar{I}_R / \bar{I}_R^2, C)$$

the *obstruction* determined by the coupling χ.

The obstruction φ will in general depend on the choice of ξ and η in (23); for these are not unique. However, according to 11.2.7, there is an isomorphism of $H^3(G, C)$ with the cokernel of the homomorphism

$$\mathrm{Hom}_G(\bar{I}_R / \bar{I}_R^2, C) \longrightarrow \mathrm{Hom}_G(I_F \bar{I}_R / \bar{I}_R^2, C). \tag{28}$$

Thus χ determines an element Δ of $H^3(G, C)$.

The important facts about Δ are as follows.

11.4.19. *Let χ be a coupling of G to N. Let ξ, η be homomorphisms as in* (23) *leading to an obstruction φ. Let J be the image of the homomorphism* (28). *Then*:

(i) *$\Delta = \varphi + J$ is independent of the choice of ξ and η*;
(ii) *by varying η we obtain all obstructions in the coset Δ.*

For a proof of 11.4.19 we refer the reader to [b29], §5.5.

It is now possible to give a formal criterion for a coupling to be realizable in an extension.

11.4.20. *Let G and N be groups and suppose that χ is a coupling of G to N. Then there is an extension of N by G with χ as its coupling if and only if χ corresponds to the zero element of $H^3(G, C)$ where C is the centre of N regarded as a G-module by means of χ.*

Proof. Suppose that χ is realized by an extension $N \rightarrowtail E \twoheadrightarrow G$. As usual let $R \rightarrowtail F \overset{\pi}{\twoheadrightarrow} G$ be a fixed presentation. There is a homomorphism $\sigma\colon F \to E$

that lifts π; thus

$$\begin{array}{ccccc} R & \rightarrowtail & F & \overset{\pi}{\twoheadrightarrow} & G \\ \downarrow & & \downarrow{\scriptstyle\sigma} & & \| \\ N & \rightarrowtail & E & \twoheadrightarrow & G \end{array}$$

is a commutative diagram. Define $\xi\colon F \to \operatorname{Aut} N$ to be the composite of σ with the conjugating homomorphism $E \to \operatorname{Aut} N$, and let η be the restriction of ξ to R. Then the diagram

$$\begin{array}{ccccc} R & \rightarrowtail & F & \overset{\pi}{\twoheadrightarrow} & G \\ {\scriptstyle\eta}\downarrow & & {\scriptstyle\xi}\downarrow & & {\scriptstyle\chi}\downarrow \\ N & \overset{\tau}{\longrightarrow} & \operatorname{Aut} N & \overset{\nu}{\twoheadrightarrow} & \operatorname{Out} N \end{array} \tag{29}$$

is commutative. This ξ and η will do very well to construct an obstruction φ.

If $f \in F$ and $r \in R$, then

$$\begin{aligned} f * r = (r^\sigma)^{-1}((r^{f^{-1}})^\sigma)^{f^\xi} &= (r^\sigma)^{-1}(f^\sigma)^{-1}(r^{f^{-1}})^\sigma f^\sigma \\ &= (r^\sigma)^{-1} r^\sigma = 1. \end{aligned}$$

Hence $\varphi = 0$ and χ corresponds to the zero element of $H^3(G, C)$. (Here one should remember that the element of $H^3(G, C)$ determined by χ does not depend on ξ and η by 11.4.19).

Conversely suppose that φ corresponds to 0 in $H^3(G, C)$. Then 11.4.19(ii) shows that ξ and η may be chosen so that (29) is commutative and $f * r = 1$ for all $f \in F$ and $r \in R$. This means that $r^\eta = ((r^{f^{-1}})^\eta)^{f^\xi}$, which, when r is replaced by r^f, becomes

$$(r^f)^\eta = (r^\eta)^{f^\xi}. \tag{30}$$

Now define $M = \{r(r^{-1})^\eta \mid r \in R\}$, a subset of $F \ltimes_\xi N = S$. By using (30) it is easy to show that the mapping $r \mapsto r(r^{-1})^\eta$ is a homomorphism of F-operator groups. Hence $M \lhd FM$. Also for x in N we have $x^{r(r^{-1})^\eta} = x^{r^\xi (r^{-1})^\xi} = x^{(rr^{-1})^\xi} = x$ since $\xi = \eta\tau$; thus $[M, N] = 1$. Therefore $M \lhd FN = S$ and $MN = M \times N = RN$, so $M \in \mathscr{M}(F, R, N, \xi)$.

Finally $N \rightarrowtail S/M \twoheadrightarrow G$ is an extension which has coupling χ. □

Extensions of Centerless Groups

Consider the case where N has trivial centre. Then $H^3(G, C) = 0$ and every coupling of G to N arises from some extension of N by G. Moreover up to equivalence there is only one such extension since $H^2(G, C) = 0$. Of course

each equivalence class of extensions gives rise to a unique coupling, as we saw in 11.1.1.

We sum up our conclusions in the following form:

11.4.21. *Let N be a group with trivial center and let G be any group. Then there is a bijection between the set of all equivalence classes of extensions of N by G and the set of all couplings of G to N.*

At the other extreme is the case where $N = C$ is abelian and χ is essentially a homomorphism from G to Aut N. We can define $\xi = \pi\chi$ and $\eta = 1$, obtaining in (29) a commutative diagram. Using this ξ and η in the definition we get $f * r = 1$ for all f and r. This means that every coupling χ corresponds to the zero element of $H^3(G, C)$, a conclusion that is hardly surprising since χ is realized by the semidirect product extension.

We mention without going into details the following additional fact. Suppose that G is a group and A a G-module. If $\Delta \in H^3(G, A)$, there exists a group N whose center is isomorphic with A, and a coupling $\chi: G \to \text{Out } N$ which is consistent with the G-module structure of A and corresponds to Δ as in 11.4.19. Of course χ is realizable by an extension of N by G if and only if $\Delta = 0$. A fuller account of the theory of obstructions may be found in [b29].

While group-theoretic interpretations of the cohomology groups in dimensions greater than 3 are known, no really convincing applications to group theory have been made.

Exercises 11.4

1. Let G be a countable locally finite group and let M be a G-module which is uniquely divisible by every prime that divides the order of an element of G. Prove that $H^n(G, M) = 0$ if $n > 1$ [use 11.3.8 and Exercise 11.3.9]. Show that $H^1(G, M)$ need not be 0 by using 11.4.7.

2. Let $N \lhd E$ and assume that $C_E(N) = \zeta N = C$ say. Put $G = E/N$ and write **e** for the extension $N \rightarrowtail E \twoheadrightarrow G$. Denote by $A(N)$ the set of all automorphisms of E that operate trivially on N and G.
   (a) Prove that $A(N)$ is an abelian group which is isomorphic with Der(G, C). [*Hint*: Show that if $\gamma \in A(N)$, then $[E, \gamma] \leq C$.]
   (b) Prove that $A(N) \cap \text{Inn } E$ maps to Inn(G, C) under the above isomorphism, and deduce that $A(N)/A(N) \cap \text{Inn } E \simeq H^1(G, C)$.

3. In the notation of the preceding problem let Aut **e** denote the group of automorphisms of E that leave N invariant. Put Out **e** = Aut **e**/Inn E. Show that there is an exact sequence

$$0 \longrightarrow H^1(G, C) \longrightarrow \text{Out } \mathbf{e} \longrightarrow \text{Out } N.$$

[*Hint*: Let $\gamma \in$ Aut **e** and consider the restriction of γ to N.]

4. (R. Ree). Let E be a noncyclic finitely generated torsion-free nilpotent group. Prove that Out E contains elements of infinite order. [*Hint*: Let N be a maximal normal abelian subgroup of E: then $N = C_E(N)$. Assuming the result false, argue that $H^1(G, N)$ is a torsion group where $G = E/N$. Now find an M such that $N \leq M$ and E/M infinite cyclic. Show that $H^1(E/M, N^M)$ is torsion and apply Exercise 11.3.2.]

5. If M is a trivial G-module, establish the existence of the *Universal Coefficients Sequence*

$$\text{Ext}(G_{\text{ab}}, M) \rightarrowtail H^2(G, M) \twoheadrightarrow \text{Hom}(M(G), M).$$

Show also that the sequence splits [*Hint*: Choose a presentation of G and apply 11.4.13 and 11.4.14.]

6. If G is a finite group, show that $M(G)$ is finite and that $M(G) \simeq H^2(G, \mathbb{C}^*)$ where $\mathbb{C}^*$ is the multiplicative group of nonzero complex numbers operated upon trivially by G. [*Hint*: Use Hopf's formula to show that $M(G)$ is finitely generated. Apply Exercise 11.3.10.]

7. Let G be an abelian group. Prove that every central extension by G is abelian if and only if $G \wedge G = 0$. Prove also that a finitely generated group has this property precisely when it is cyclic.

*8. If G is an elementary abelian group of order p^n, then $M(G)$ is elementary abelian of order $p^{\binom{n}{2}}$.

9. If G is free abelian of rank n, then $M(G)$ is free abelian of rank $\binom{n}{2}$.

10. According to 11.4.18 a central extension $C \rightarrowtail E \twoheadrightarrow G$ determines a homomorphism $\delta\colon M(G) \to C$ called the *differential*. Prove that $\text{Im}\,\delta = E' \cap C$. Deduce that δ is surjective if and only if $C \leq E'$. (Such an extension is called a *stem extension*.) [*Hint*: The given extension is equivalent to one of the form $C \rightarrowtail (C \times F)/R^{\varphi'} \twoheadrightarrow G$ where $R \rightarrowtail F \twoheadrightarrow G$ is a presentation of G and $\varphi \in \text{Hom}_F(R, C)$.]

11. Prove that Schur's theorem (10.1.4) is equivalent to the assertion that $M(G)$ is finite whenever G is finite. (Use Exercise 11.4.10.)

12. A central extension $C \rightarrowtail E \twoheadrightarrow G$ is called a *stem cover* of G if its differential is an isomorphism. Prove that every stem cover of G is isomorphic to a stem cover $M(G) \rightarrowtail E \twoheadrightarrow G$ with differential equal to 1. [*Hint*: Let $\varphi \in \text{Hom}(R/[R, F], C)$ determine the given stem cover, $R \rightarrowtail F \twoheadrightarrow G$ being a presentation of G. If δ is the differential of a stem cover $C \rightarrowtail E \twoheadrightarrow G$, consider $\varphi\delta^{-1} \in \text{Hom}(R/[R, F], M(G))$.]

13. Prove that every stem extension is an image of a stem cover (i.e., there is a morphism $(\alpha, \beta, 1)$ from a stem cover with α and β surjective).

14. Prove that there is a bijection between the set of isomorphism classes of stem covers of G and $\text{Ext}(G_{\text{ab}}, M(G))$. Construct four non-isomorphic stem covers of $\mathbb{Z}_2 \times \mathbb{Z}_2$. [Use Exercise 11.4.13.]

15. A finite group G has a unique isomorphism class of stem covers if and only if $(|G_{\text{ab}}|, |M(G)|) = 1$.

*16. (a) Establish the naturality of the 5-term homology sequence (see 11.4.17). [*Hint*: Start with presentations $R \rightarrowtail F \twoheadrightarrow E$ and $\bar{R} \rightarrowtail \bar{F} \twoheadrightarrow \bar{E}$ and lift $\gamma: G \to \bar{G}$ to $\xi: F \to \bar{F}$.]

(b) Prove also that $(\gamma\bar{\gamma})_* = \gamma_*\bar{\gamma}_*$ where $\gamma: G \to \bar{G}$ and $\bar{\gamma}: \bar{G} \to \bar{\bar{G}}$ are homomorphisms. (In the language of category theory this says that $M(-)$ is a functor.) [*Hint*: Show that γ_* does not depend on the particular lifting ξ.]

17. Let G be the group with generators $x_1, x_2, \ldots, x_n$ and defining relations $[x_1, x_2] = [x_2, x_3] = \cdots = [x_{n-1}, x_n] = 1$. Using Hopf's formula, show that $M(G)$ is free abelian of rank $n - 1$.

CHAPTER 12

Generalizations of Nilpotent and Soluble Groups

In Chapter 5 we found numerous properties of finite groups which are equivalent nilpotence—see especially 5.2.4. For example, normality of all the Sylow subgroups is such a property. When applied to infinite groups, these properties are usually much weaker, giving rise to a series of wide generalizations of nilpotence. For soluble groups the situation is similar. The aim of this chapter is to discuss the main types of generalized nilpotent and soluble groups and their interrelations.

12.1. Locally Nilpotent Groups

If $\mathscr{P}$ is a property of groups, a group G is called a *locally $\mathscr{P}$-group* if each finite subset of G is contained in a $\mathscr{P}$-subgroup of G. If the property $\mathscr{P}$ is inherited by subgroups, this is equivalent to the requirement that each finitely generated subgroup have $\mathscr{P}$.

Our first class of generalized nilpotent groups is the class of *locally nilpotent groups*. It is easy to see that images and subgroups of a locally nilpotent group are locally nilpotent. There are certain properties of nilpotent groups which are of a local character in the sense that they are statements about finite sets of elements; such properties are inherited by locally nilpotent groups. For example, there is the following result.

12.1.1. *Let G be a locally nilpotent group. Then the elements of finite order in G form a fully-invariant subgroup T (the torsion-subgroup of G) such that G/T is torsion-free and T is a direct product of p-groups.*

This follows immediately from 5.2.7. Note that infinite p-groups are not in general nilpotent (Exercise 5.2.11), or in fact even locally nilpotent by a famous example of Golod [a59].

One rather obvious way of constructing locally nilpotent groups is to take the direct product of a family of nilpotent groups: if the nilpotent classes of the direct factors are unbounded, the resulting group will be a non-nilpotent locally nilpotent group.

Products of Normal Locally Nilpotent Subgroups

Recall that the product of two normal nilpotent subgroups is nilpotent—this is Fitting's Theorem (5.2.8). The corresponding statement holds for locally nilpotent groups and is of great importance.

12.1.2 (The Hirsch–Plotkin Theorem). *Let H and K be normal locally nilpotent subgroups of a group. Then the product $J = HK$ is locally nilpotent.*

Proof. Choose a finitely generated subgroup of J, say $\langle h_1 k_1, \dots, h_m k_m \rangle$ where $h_i \in H$ and $k_i \in K$. We must prove that J is nilpotent. To this end we introduce the subgroups $X = \langle h_1, \dots, h_m \rangle$ and $Y = \langle k_1, \dots, k_m \rangle$, and also $Z = \langle X, Y \rangle$. Since $J \leq Z$, it is enough to show that Z is nilpotent.

Let C denote the *set* of all commutators $[h_i, k_j]$, $i, j = 1, \dots, m$; then $C \subseteq H \cap K$ since H and K are normal. Hence $\langle X, C \rangle$ is a finitely generated subgroup of H, so in fact $\langle X, C \rangle$ is nilpotent. Since finitely generated nilpotent groups satisfy the maximal condition (5.2.17), the normal closure C^X is finitely generated, as well as being nilpotent. Moreover $C^X \leq H \cap K$, so that $\langle Y, C^X \rangle \leq K$. Therefore $\langle Y, C^X \rangle$ is nilpotent and finitely generated, whence it satisfies the maximal condition. Now $[X, Y] = C^{XY}$ by 5.1.7. Thus, using 5.1.6, we have

$$\langle Y, C^X \rangle = \langle Y, C^{XY} \rangle = \langle Y, [X, Y] \rangle = Y^X.$$

It follows that Y^X is nilpotent, and by symmetry X^Y is nilpotent. Finally $Z = \langle X, Y \rangle = X^Y Y^X$ is nilpotent by Fitting's Theorem. □

12.1.3. *In any group G there is a unique maximal normal locally nilpotent subgroup (called the Hirsch–Plotkin radical) containing all normal locally nilpotent subgroups of G.*

Proof. It is easy to see that the union of a chain of locally nilpotent subgroups is locally nilpotent. Thus Zorn's Lemma can be applied to show that each normal locally nilpotent subgroup is contained in a maximal normal locally nilpotent subgroup. If H and K are two maximal normal locally nilpotent subgroups of G, then HK is locally nilpotent by 12.1.2. Hence $H = K$. □

The reader will observe that the Fitting subgroup is always contained in the Hirsch–Plotkin radical. Of course these subgroups will coincide if the group is finite.

Ascendant Subgroups

Before proceeding further with the theory of locally nilpotent groups we shall introduce a very useful generalization of a subnormal subgroup called an ascendant subgroup.

By an *ascending series* in a group G we shall mean a set of subgroups $\{H_\alpha | \alpha < \beta\}$ indexed by ordinals less than an ordinal β such that:

(a) $H_{\alpha_1} \leq H_{\alpha_2}$ if $\alpha_1 \leq \alpha_2$;
(b) $H_0 = 1$ and $G = \bigcup_{\alpha<\beta} H_\alpha$;
(c) $H_\alpha \lhd H_{\alpha+1}$;
(d) $H_\lambda = \bigcup_{\alpha<\lambda} H_\alpha$ if λ is a limit ordinal.

Condition (d) is inserted to ensure completeness of the series under unions. It is often convenient to write the ascending series in the form

$$1 = H_0 \lhd H_1 \lhd \cdots H_\beta = G.$$

Of course the H_α are the *terms* of the series, while the $H_{\alpha+1}/H_\alpha$ are the *factors*: the ordinal β is the *length* or *ordinal type*. Should β be finite, the ascending series becomes a familiar object, a series of finite length. Sometimes it is convenient to speak of an ascending series *beginning at a subgroup* K: in this case $H_0 = K$ but (a)–(d) are otherwise unchanged.

A subgroup which occurs in some ascending series of a group G is called an *ascendant subgroup*; this is an evident generalization of a subnormal subgroup. It may be as well to give an example at this point.

Let $G = X \ltimes A$ be a so-called *locally dihedral* 2-*group*; this means that A is of type 2^∞, while $X = \langle x \rangle$ has order 2 and $a^x = a^{-1}$, $(a \in A)$. Let A_i be the unique (cyclic) subgroup of A with order 2^i. Then $[A_{i+1}, X] = A_{i+1}^2 = A_i$ since $[a, x] = a^{-2}$. Consequently $XA_i \lhd XA_{i+1}$ and there is an ascending series $X \lhd XA_1 \lhd XA_2 \lhd \cdots \lhd XA = G$; notice that $\bigcup_{i<\omega} XA_i = XA$ here. Hence X is ascendant in G. On the other hand, $X^G = X^A = X[A, X] = XA = G$, so X is not subnormal in G.

Returning now to locally nilpotent groups, we shall show that the Hirsch–Plotkin radical contains many more than just the *normal* locally nilpotent subgroups.

12.1.4. *If G is any group, the Hirsch–Plotkin radical contains all the ascendant locally nilpotent subgroups.*

Proof. Let H be an ascendant locally nilpotent subgroup of G. Then there is an ascending series $H = H_0 \lhd H_1 \lhd \cdots H_\beta = G$. Define $\bar{H}_\alpha$ to be H^{H_α};

then one quickly verifies that

$$H = \bar{H}_1 \lhd \bar{H}_2 \lhd \cdots \bar{H}_\beta = H^G$$

is an ascending series. We argue by transfinite induction that $\bar{H}_\alpha$ is locally nilpotent. If this is false, there is a first ordinal α such that $\bar{H}_\alpha$ is not locally nilpotent. If α were a limit ordinal, $\bar{H}_\alpha$ would equal $\bigcup_{\gamma<\alpha} \bar{H}_\gamma$ and, $\bar{H}_\gamma$ being locally nilpotent for $\gamma < \alpha$, it would follow that $\bar{H}_\alpha$ is locally nilpotent. Hence α cannot be a limit ordinal, $\alpha - 1$ exists and $\bar{H}_{\alpha-1}$ is locally nilpotent. Now $(\bar{H}_{\alpha-1})^{H_\alpha} = (H^{H_{\alpha-1}})^{H_\alpha} = H^{H_\alpha} = \bar{H}_\alpha$: moreover for any x in H_α we have $\bar{H}_{\alpha-1}^x \lhd \bar{H}_\alpha^x = \bar{H}_\alpha$. Consequently $\bar{H}_\alpha$ is a product of normal locally nilpotent subgroups and is therefore locally nilpotent by 12.1.3. By this contradiction $\bar{H}_\beta = H^G$ is locally nilpotent, which shows that H^G, and hence H, is contained in the Hirsch–Plotkin radical of G. □

Maximal Subgroups and Principal Factors in Locally Nilpotent Groups

We recall two known properties of nilpotent groups: maximal subgroups are normal and principal factors are central (5.2.4 and 5.2.2). Let us show that these hold for locally nilpotent groups.

12.1.5 (Baer, McLain). *If M is a maximal subgroup of a locally nilpotent group G, then M is normal in G. Equivalently $G' \leq$ Frat G.*

Proof. If M is not normal, then $G' \nleq M$ and there is an element c in $G' \backslash M$. Then $G = \langle c, M \rangle$ because M is maximal. Now $c \in \langle g_1, \ldots, g_n \rangle'$ for certain $g_1, \ldots, g_n$, and these elements all belong to $L = \langle c, F \rangle$ for a suitable finitely generated subgroup F of M. Since $c \notin F$, we can use 3.3.14 to find a subgroup N of L which is maximal subject to containing F but not c. A subgroup of L which is larger than N would contain c as well as F and hence would have to equal L; this amounts to saying that N is a maximal subgroup of the nilpotent group L. Hence $N \lhd L$ and L/N is abelian. However this leads to $c \in L' \leq N$, in contradiction to the choice of N. □

For finite groups the condition $G' \leq$ Frat G is equivalent to nilpotence. However for infinite groups this is a very weak property because an infinite group may not have any maximal subgroups and $G =$ Frat G is a real possibility. For example, let G be the standard wreath product of groups of type p^∞ and q^∞: it is an easy exercise (see Exercise 12.1.8) to show that $G =$ Frat G, so that certainly $G' \leq$ Frat G. However G is not locally nilpotent if $p \neq q$. Thus $G' \leq$ Frat G does not imply local nilpotence.

12.1.6 (Mal'cev, McLain). *A principal factor of a locally nilpotent group G is central.*

Proof. Let N be a minimal normal subgroup of G. It suffices to prove that N is central in G. If $N \nleq \zeta G$, there exist a in N and g in G such that $b = [a, g] \neq 1$. Since $b \in N$, we have $N = b^G$ by minimality of N. Hence $a \in \langle b^{g_1}, \ldots, b^{g_n} \rangle$ for certain g_i in G. Let $H = \langle a, g, g_1, \ldots, g_n \rangle$, a nilpotent group, and set $A = a^H$. Then $b \in [A, H]$, so that $b^{g_i} \in [A, H]$ and consequently $a \in [A, H]$. Hence $A = [A, H]$ and $A = [A, {}_rH]$ for all r. Since H is nilpotent, it follows that $A = 1$ and $a = 1$. But this means that $b = [a, g] = 1$. □

Locally Nilpotent Groups Subject to Finiteness Conditions

Sometimes when a finiteness restriction is placed upon a locally nilpotent group, the group is forced to become nilpotent. An obvious example is: every finitely generated locally nilpotent group is nilpotent. Here is a less trivial result of the same kind.

12.1.7 (McLain). *If the locally nilpotent group G satisfies the maximal condition on normal subgroups, then G is a finitely generated nilpotent group.*

Proof. Clearly G/G' satisfies max-n and hence max since it is an abelian group. Therefore $G = XG'$ for some finitely generated subgroup X. Then X is nilpotent of class c, say. Let "bars" denote quotient groups modulo $\gamma_{c+2}G$. Thus $\bar{G} = \bar{X}\bar{G}'$ and $\bar{G}$ is nilpotent. Therefore $\bar{G}' \leq \text{Frat } \bar{G}$ by 5.2.16 and $\bar{G} = \bar{X}(\text{Frat } \bar{G})$. But $\text{Frat } \bar{G}$ is finitely generated, by 5.2.17, and its generators are nongenerators of $\bar{G}$ by 5.2.12. Hence $\bar{G} = \bar{X}$, which means that $\bar{G}$ has nilpotent class at most c and $\gamma_{c+1}G = \gamma_{c+2}G$. Writing L for $\gamma_{c+1}G$, we have $L = [L, G]$. If $L \neq 1$, then by max-n there is a normal subgroup N of G which is maximal subject to $N < L$. But L/N is minimal normal in G/N, so it is central by 12.1.6. Thus $[L, G] \leq N < L$, a contradiction. Hence $L = 1$ and G is nilpotent. □

Notice the corollary: max and max-n are the same property for locally nilpotent groups.

If one imposes min-n, the minimal condition on normal subgroups, on a locally nilpotent group, hoping for nilpotence, one is disappointed. For example, let $G = X \ltimes A$ be a locally dihedral 2-group. This group is locally nilpotent and even satisfies min. However $G' = A = [A, G]$, so the lower central series terminates at G' and G cannot be nilpotent.

Nevertheless a fairly good description of the structure of locally nilpotent groups with min-n can be given.

12.1.8 (McLain). *A locally nilpotent group G satisfies the minimal condition on normal subgroups if and only if it is the direct product of finitely many Černikov p-groups for various primes p.*

Proof. Let G satisfy min-n. According to 5.4.22 there exists a unique minimal subgroup F with finite index in G. Furthermore F satisfies min-n by 3.1.8. Now if F is abelian, it satisfies min and by the structure theorem for abelian groups with min (4.2.11), F is divisible—bear in mind that F cannot have a proper subgroup with finite index. In this case G is a Černikov group; also G is the direct product of its p-components by 12.1.1. Henceforth assume that F is not abelian.

By 12.1.6 minimal normal subgroups of F are contained in ζF; thus min-n guarantees that $\zeta F \neq 1$. Moreover $\zeta F \neq F$, so that $\zeta F < \zeta_2 F$ by the same argument. Let $x \in \zeta_2 F$ and $y \in F$; then $x^y = xz$ for some z in ζF. Now ζF has min because F has min-n, and $\zeta_2 F/\zeta F$ has min for the same reason. Therefore x and z have finite orders: what is more, $|z|$ divides $|x|$. Regard x as fixed and y as variable. Since ζF contains only finitely many elements of each given order, there are only finitely many conjugates of x in F. Hence $|F : C_F(x)|$ is finite, $F = C_F(x)$ and $x \in \zeta F$. However this contradicts $\zeta F < \zeta_2 F$.

The converse is left to the reader as an exercise. □

It is an immediate corollary that min and min-n are the same property for locally nilpotent groups.

McLain's Characteristically Simple Groups

We shall describe next some famous examples due to D.H. McLain of locally nilpotent groups that are characteristically simple. These groups are perfect and have trivial center, which should convince the reader that locally nilpotent groups are far removed from the familiar realm of nilpotent groups.

In essence McLain's groups are infinite analogues of unitriangular matrix groups (see 5.1). We begin with $\mathbb{Q}$, the ordered set of rational numbers, and any field F, and we form a vector space V with countably infinite dimension over F: let $\{v_\lambda | \lambda \in \mathbb{Q}\}$ be a basis for V. If $\lambda < \mu$, denote by $e_{\lambda\mu}$ the usual elementary linear transformation of V: thus

$$v_\lambda e_{\lambda\mu} = v_\mu \qquad \text{and} \qquad v_\nu e_{\lambda\mu} = 0 \qquad (\nu \neq \lambda).$$

The standard multiplication rules hold for these $e_{\lambda\mu}$:

$$e_{\lambda\mu} e_{\mu\nu} = e_{\lambda\nu} \qquad \text{and} \qquad e_{\lambda\mu} e_{\nu\xi} = 0 \qquad (\mu \neq \nu). \tag{1}$$

In particular $e_{\lambda\mu}^2 = 0$, from which it follows that $(1 + ae_{\lambda\mu})^{-1} = 1 - ae_{\lambda\mu}$ for a in F. Using this rule for inverses and also (1) we calculate that

$$\left.\begin{aligned} &[1 + ae_{\lambda\mu}, 1 + be_{\mu\nu}] = 1 + abe_{\lambda\nu} \\ \text{and} \quad &[1 + ae_{\lambda\mu}, 1 + be_{\nu\zeta}] = 1 \quad \text{if} \quad \lambda \neq \zeta \quad \text{and} \quad \mu \neq \nu. \end{aligned}\right\} \tag{2}$$

McLain's group is the group of linear transformations of V generated by all $1 + ae_{\lambda\mu}$ where $a \in F$ and $\lambda < \mu \in \mathbb{Q}$. Let this be written

$$M = M(\mathbb{Q}, F).$$

One sees from the multiplication rules (1) that every element of M can be written uniquely in the form $1 + \sum_{\lambda<\mu} a_{\lambda\mu}e_{\lambda\mu}$ where $a_{\lambda\mu} \in F$ and almost all of the $a_{\lambda\mu}$ are zero. Conversely any element x of this form belongs to M. To prove this we assume that $x \neq 1$ and choose $\mu_0 \in \mathbb{Q}$ as large as possible subject to $a_{\lambda_0\mu_0} \neq 0$ for some λ_0. Write $u = a_{\lambda_0\mu_0}e_{\lambda_0\mu_0}$ and $v = x - u - 1$. Then of course $x = 1 + u + v = (1 + u)(1 + v)$; for $uv = 0$ because $a_{\mu_0\mu_1} = 0$ if $\mu_0 < \mu_1$. By induction on the number of nonzero terms in x we have $1 + v \in M$, so that $x \in M$ as claimed.

The following theorem lists the essential properties of McLain's group.

12.1.9 (McLain). *Let* $M = M(\mathbb{Q}, F)$.

(i) *M is the product of its normal abelian subgroups, so M is locally nilpotent.*
(ii) *If F has characteristic $p > 0$, then M is a p-group: if F has characteristic 0, then F is torsion-free.*
(iii) *M is characteristically simple.*
(iv) *$\zeta M = 1$ and $M = M'$.*

Proof. (i) By the commutator relations (2) each conjugate of $1 + ae_{\lambda\mu}$ belongs to the subgroup generated by all $1 + be_{\nu\zeta}$ where $b \in F$ and $\nu \leq \lambda < \mu \leq \zeta$; therefore all conjugates of $1 + ae_{\lambda\mu}$ commute and thus $(1 + ae_{\lambda\mu})^M$ is an abelian group. Clearly M is the product of all the $(1 + ae_{\lambda\mu})^M$. Thus M equals its Hirsch–Plotkin radical and is locally nilpotent.

(ii) If $x \in M$, there exists a finite set of elements $\lambda_1, \dots, \lambda_n$ in $\mathbb{Q}$ such that $\lambda_1 < \cdots < \lambda_n$ and x belongs to the subgroup H generated by all $1 + ae_{\lambda_i\lambda_{i+1}}$, $i = 1, \dots, n - 1$, $a \in F$. Clearly the mapping $1 + ae_{\lambda_i\lambda_{i+1}} \mapsto 1 + aE_{ii+1}$ establishes an isomorphism between H and the unitriangular group $U(n, F)$; both assertions now follow from the discussion of the unitriangular group in 5.1.

(iii) Suppose that N is characteristic in M and $N \neq 1$. We need to prove that $N = M$. The first step is to show that N contains a generator of M. If $1 \neq x \in N$, then $x \in H$ where H is a unitriangular group as in (ii). Also $1 \neq H \cap N \lhd H$, so that $\zeta H \cap N \neq 1$ by 5.2.1. Now the center of $U(n, F)$ consists of all $1 + aE_{1n}$, $a \in F$ (Exercise 5.1.13): consequently some $1 + ae_{\lambda_1\lambda_n}$ with $a \neq 0$ belongs to N as claimed.

Now let $\lambda < \mu$ be a pair of rational numbers. It is a well-known fact that there exists an order-preserving permutation α of $\mathbb{Q}$ such that $\lambda\alpha = \lambda_1$ and $\mu\alpha = \lambda_n$. Moreover α determines an automorphism of M given by $1 + be_{\nu\xi} \mapsto 1 + be_{\nu\alpha\xi\alpha}$. Since N is characteristic in M, it follows that N contains $1 + ae_{\lambda\mu}$ for all $\lambda < \mu$ in $\mathbb{Q}$. Finally, if $b \in F$, then N also contains

$$[1 + ae_{\lambda\mu}, 1 + a^{-1}be_{\mu\nu}] = 1 + be_{\lambda\nu}$$

for all $\lambda < \nu$ in $\mathbb{Q}$. Therefore $N = M$ and M is characteristically simple.

(iv) By (iii) $\zeta M = 1$ or M: obviously M is not abelian, so $\zeta M = 1$. For a similar reason $M' = M$. □

Exercises 12.1

1. A soluble p-group is locally nilpotent.
2. A group is called *radical* if it has an ascending series with locally nilpotent factors. Define the *upper Hirsch–Plotkin series* of a group G to be the ascending series $1 = R_0 \leq R_1 \leq \cdots$ in which $R_{\alpha+1}/R_\alpha$ is the Hirsch–Plotkin radical of G/R_α and $R_\lambda = \bigcup_{\alpha<\lambda} R_\alpha$ for limit ordinals λ. Prove that the radical groups are precisely those groups which coincide with a term of their upper Hirsch–Plotkin series.
3. Let G be a radical group and H is Hirsch–Plotkin radical.
   (a) If $1 \neq N \lhd G$, show that $H \cap N \neq 1$.
   (b) Prove that $C_G(H) = \zeta H$.
4. Show that a radical group with finite Hirsch–Plotkin radical is finite and soluble.

*5. Write H asc K to mean that H is an ascendant subgroup of a group K. Establish the following properties of ascendant subgroups.
   (a) H asc K and K asc G imply that H asc G.
   (b) H asc $K \leq G$ and L asc $M \leq G$ imply that $H \cap L$ asc $K \cap M$.
   (c) If H asc $K \leq G$ and α is a homomorphism from G, then H^α asc K^α. Deduce that HN asc KN if $N \lhd G$.

6. An ascending series that contains all the terms of another ascending series is called a *refinement* of it. An *ascending composition series* is an ascending series with no refinements other than itself. Characterize ascending composition series in terms of their factors and prove a version of the Jordan–Hölder Theorem for such series.
7. (Baer). Show that a nilpotent group with min-n is a Černikov group whose center has finite index. Show also that the derived subgroup is finite. (See also 12.2.9).
8. Let G be the standard wreath product of two quasicyclic groups. Prove that $G = \text{Frat } G$.
9. Establish the commutator relations (2).
10. Prove that $M(\mathbb{Q}, F)$ has no proper subgroups of finite index and no nontrivial finitely generated normal subgroups. Identify the Frattini subgroup.
11. Need a cartesian product of finite p-groups be locally nilpotent?

12.2. Some Special Types of Locally Nilpotent Groups

In this section we shall consider some natural generalizations of nilpotence that are stronger than local nilpotence.

The Normalizer Condition

Recall that a group satisfies the *normalizer condition* if each proper subgroup is smaller than its normalizer. It was shown (in 5.2.4) that for finite groups the normalizer condition is equivalent to nilpotence. It is not difficult to see that the normalizer condition can be reformulated in terms of ascendance.

12.2.1. *A group G satisfies the normalizer condition if and only if every subgroup is ascendant.*

Proof. Let G satisfy the normalizer condition. For any subgroup H one may define a chain of subgroups $\{H_\alpha\}$ by the rules

$$H_0 = H, \qquad H_{\alpha+1} = N_G(H_\alpha), \qquad \text{and} \qquad H_\lambda = \bigcup_{\beta<\lambda} H_\beta$$

where α is an ordinal and λ a limit ordinal. If $H_\alpha < H_{\alpha+1}$ for all α, it would follow that $|G|$ is not less than the cardinality of α for all α, obviously absurd. Hence $H_\alpha = H_{\alpha+1}$ for some α, so that $H_\alpha = G$ by the normalizer condition. Since the H_α's form an ascending series from H, it follows that H is ascendant in G.

Conversely assume that every subgroup of G is ascendant and let $H < G$. Then there is an ascending series $H = H_0 \lhd H_1 \lhd H_2 \lhd \cdots H_\beta = G$. By omitting redundant terms we may assume that $H \neq H_1$. Hence $H_1 \leq N_G(H)$ and $H \neq N_G(H)$. □

Now that we have a clearer idea of what the normalizer condition entails, let us relate this property to local nilpotence.

12.2.2 (Plotkin). *If a group G satisfies the normalizer condition, then it is locally nilpotent.*

Proof. Let $g \in G$; then $\langle g \rangle$ is ascendant in G by 12.2.1, while by 12.1.4 the subgroup $\langle g \rangle$ is contained in H, the Hirsch–Plotkin radical of G. Therefore $H = G$ and G is locally nilpotent. □

McLain's group $M(\mathbb{Q}, F)$ is an example of a locally nilpotent group that does *not* satisfy the normalizer condition (Exercise 12.2.8). A simpler example is $W = H \wr K$ where $|H| = p$ and K is an infinite elementary abelian p-group; here K is self-normalizing.

Hypercentral Groups

An ascending series $1 = G_0 \lhd G_1 \lhd \cdots G_\beta = G$ in a group G is said to be *central* if $G_\alpha \lhd G$ and $G_{\alpha+1}/G_\alpha$ lies in the center of G/G_α for every $\alpha < \beta$. A group which possesses a central ascending series is called *hypercentral.*

This natural class of generalized nilpotent groups can also be characterized in terms of the *transfinitely extended upper central series*, which is defined in the following manner. If G is any group and α an ordinal, the terms $\zeta_\alpha G$ of the upper central series of G are defined by the usual rules

$$\zeta_0 G = 1 \qquad \text{and} \qquad \zeta_{\alpha+1} G/\zeta_\alpha G = \zeta(G/\zeta_\alpha G)$$

together with the completeness condition

$$\zeta_\lambda G = \bigcup_{\alpha<\lambda} \zeta_\alpha G$$

where λ is a limit ordinal. Since the cardinality of G cannot be exceeded, there is an ordinal β such that $\zeta_\beta G = \zeta_{\beta+1} G =$, etc., a terminal subgroup called the *hypercenter* of G. It is sometimes convenient to call $\zeta_\alpha G$ the *α-center* of G.

12.2.3. *A group is hypercentral if and only if it coincides with its hypercenter.*

The easy proof is left to the reader. As examples of hypercentral groups we cite the locally dihedral 2-group and any direct product of nilpotent groups.

How is hypercentrality related to local nilpotence? The answer is given by

12.2.4. *A hypercentral group G satisfies the normalizer condition and hence is locally nilpotent.*

Proof. Let $\{G_\alpha | \alpha \leq \beta\}$ be a central ascending series of G and let $H \leq G$. Since $G_{\alpha+1}/G_\alpha$ is central in G, we have $HG_\alpha \lhd HG_{\alpha+1}$ for all α. Hence $HG_0 = H$ is ascendant in $HG_\beta = G$. The result now follows from 12.2.1 and 12.2.2. □

For many years it was not known if a group with the normalizer condition was automatically hypercentral. This was finally shown to be false by Heineken and Mohamed in 1968—see [a88] and [a83].

12.2.5. *A locally nilpotent group with the minimal condition on normal subgroups is hypercentral.*

This follows from 12.1.6.

Baer Groups and Gruenberg Groups

The next two types of generalized nilpotent groups are characterized by the subnormality or ascendance of finitely generated subgroups. The following result is basic.

12.2.6. *Let H and K be finitely generated nilpotent subgroups of a group G and write $J = \langle H, K \rangle$.*

(i) (Gruenberg). *If H and K are ascendant in G, then J is ascendant and nilpotent.*
(ii) (Baer). *If H and K are subnormal in G, then J is subnormal and nilpotent.*

Proof. (i) By 12.1.4 both H and K lie inside R, the Hirsch–Plotkin radical of G: hence $J \leq R$. Since J is plainly finitely generated, we conclude that it is nilpotent.

To prove that J is ascendant in G is harder. Let $H = H_0 \lhd H_1 \lhd \cdots H_\alpha = G$ be an ascending series with $\alpha > 0$. Keeping in mind that J is a finitely generated nilpotent group, we note that H^J is finitely generated. If α is a limit ordinal, it must follow that $H^J \leq H_\beta$ for some $\beta < \alpha$. Transfinite induction on α yields the ascendance of H^J in H_β and hence in G. If, on the other hand, α is not a limit ordinal, then $H \leq H_{\alpha-1} \lhd H_\alpha = G$ and $H^J \leq H_{\alpha-1}$: again transfinite induction leads to H^J being ascendant in G. What this argument demonstrates is that H can be replaced by H^J. In short we can suppose that $H \lhd J$ and $J = HK$.

Next we pass to a modified ascending series, defining $\bar{H}_\alpha$ to be H^{H_α}; then $H = \bar{H}_0 = \bar{H}_1 \lhd \bar{H}_2 \lhd \cdots \bar{H}_\alpha = H^G$ is an ascending series. But what is really required is another ascending series, with K-admissible terms. Such a series can be obtained by writing

$$H_\beta^* = \bigcap_{k \in K} (\bar{H}_\beta)^k.$$

It is fairly clear that $H = H_0^* = H_1^*$ and $H^G = H_\alpha^*$; also $H_\beta^* \lhd H_{\beta+1}^*$. However to conclude that the H_β^*'s form an ascending series we must prove completeness,

$$H_\lambda^* = \bigcup_{\beta < \lambda} H_\beta^*$$

for limit ordinals λ. One inclusion, $H_\lambda^* \geq \bigcup_{\beta < \lambda} H_\beta^*$, is of course obvious. To establish the other inclusion choose x from H_λ^*. Clearly $\langle x, K \rangle \leq \langle \bar{H}_\lambda, K \rangle$, which is contained in the Hirsch–Plotkin radical of G (since H^G and K are). Now $\langle x, K \rangle$ is finitely generated, so it is nilpotent and x^K is finitely generated. But $x^K \leq (H_\lambda^*)^K = H_\lambda^* \leq \bar{H}_\lambda = \bigcup_{\beta < \lambda} \bar{H}_\beta$ and the $\bar{H}_\beta$'s form an ascending series. Consequently $x^K \leq \bar{H}_\beta$ for some $\beta < \lambda$; therefore $x^K \leq H_\beta^*$ and in particular $x \in H_\beta^*$. This settles the point at issue.

The remainder of the proof is easy. For each $\beta < \alpha$ we have $H_\beta^* \lhd H_{\beta+1}^* K$ and K is ascendant in $H_{\beta+1}^* K$; hence $H_\beta^* K$ is ascendant in $H_{\beta+1}^* K$ by Exercise 12.1.5. Putting these relations together for all β, we deduce that $J = H_0^* K$ is ascendant in $H_\alpha^* K = H^G K$ and hence in G since $H^G K$ is ascendant in G.

(ii) The same method applies in this case, but it is easier since, of course, we need not consider limit ordinals. □

The following statements are immediate corollaries of 12.2.6.

12.2.7. *If every cyclic subgroup of a group is ascendant, then every finitely generated subgroup is ascendant and nilpotent.*

12.2.8. *If every cyclic subgroup of a group is subnormal, then every finitely generated subgroup is subnormal and nilpotent.*

Definitions. A group is called a *Gruenberg group* if every cyclic subgroup is ascendant and a *Baer group* if every cyclic subgroup is subnormal. Obviously every Baer group is a Gruenberg group, and by 12.2.7 every Gruenberg group is locally nilpotent. Notice also that a group with the normalizer condition is a Gruenberg group in view of 12.2.1.

The structure of Baer groups—and hence of nilpotent groups—with min-*n* is described by the following result:

12.2.9. *If G is a Baer group satisfying the minimal condition on normal subgroups, then G is nilpotent and its center has finite index.*

Proof. We know from 12.1.8 that G is a Černikov group. Let N denote the smallest normal subgroup of finite index in G. Of course, N is a divisible abelian group. It suffices to prove that N is contained in the center of G. If this is false, we can find an element g such that $[N, g] \neq 1$. Now $\langle g \rangle$ is subnormal in G, so there is a series $\langle g \rangle = H_0 \lhd H_1 \lhd \cdots \lhd H_r = G$. Then $[N, g] \leq H_{r-1}$, $[N, {}_2g] \leq H_{r-2}$, etc., and finally $[N, {}_rg] \leq \langle g \rangle$. Hence $[N, {}_{r+1}g] = 1$. If r is the smallest such integer, then $r \geq 1$. Let $M = [N, {}_{r-1}g]$ and put $m = |g|$. Since $[M, g, g] = 1$, we can use one of the fundamental commutator identities to show that $[M, g]^m = [M, g^m] = 1$. But the mapping $a \mapsto [a, {}_rg]$ is an endomorphism of N; therefore $[M, g] = [N, {}_rg]$ is divisible. Consequently, $[M, g] = 1$ in contradiction to the choice of r. □

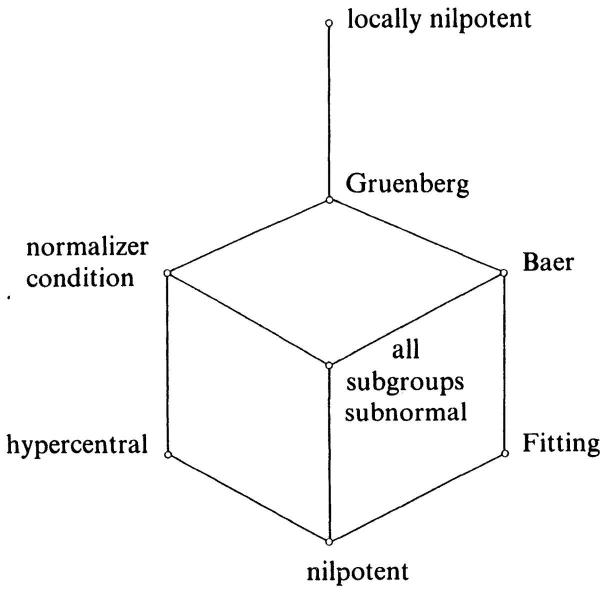
Two further classes of locally nilpotent groups will be briefly mentioned. A group G is a *Fitting group* if $G = \text{Fit } G$, that is, if G is a product of normal nilpotent subgroups. For example, McLain's group is a Fitting group. If $x \in G = \text{Fit } G$, then x lies in a product of finitely many normal nilpotent subgroups, and hence in a normal nilpotent subgroup by Fitting's theorem. Thus we have an alternative description of Fitting groups.

12.2.10. *A group G is a Fitting group if and only if every element is contained in a normal nilpotent subgroup. Every Fitting group is a Baer group.*

Lastly, a class of groups about which very little is known, groups in which every subgroup is subnormal. Obviously such groups are Baer groups and by 12.2.2 they satisfy the normalizer condition. We mention in this connection a notable theorem of Roseblade [a174]; *if every subgroup of*

a group is subnormal in a bounded number of steps, the group is nilpotent. This contrasts with the example of a non-nilpotent group with every subgroup subnormal constructed by Heineken and Mohammed [a88]. Finally Möhres has recently shown that if every subgroup of a group is subnormal, then the group is soluble.

Diagram of Group Classes



It is known that all these eight classes are distinct—see [b54] for details.

Exercises 12.2

1. If G is a hypercentral group and $1 \neq N \lhd G$, then $N \cap \zeta G \neq 1$.
2. (Baer). A group is hypercentral if and only if every nontrivial quotient group has nontrivial center.
3. A nontrivial hypercentral group cannot be perfect.
4. If A is a maximal normal abelian subgroup of a hypercentral group G, then $A = C_G(A)$.
5. (P. Hall). The product of two normal hypercentral subgroups is hypercentral.
6. If G is hypercentral and G_{ab} is a torsion group, show that G is a torsion group. Does this hold for locally nilpotent groups?
7. Give an example of a hypercentral group that is not a Baer group.

8. Prove that $M(\mathbb{Q}, F)$ does not satisfy the normalizer condition. Deduce that Fitting groups need not satisfy this condition. [*Hint*: Consider the subgroup generated by all $1 + ae_{\lambda\mu}$ where $a \in F$ and either $\lambda < \mu \leq 0$ or $0 < \lambda < \mu$.]

9. A countable locally nilpotent group is a Gruenberg group. (This is false for uncountable groups—see [b54].)

10. Prove 12.2.6(ii).

11. What is the effect on the diagram of classes of locally nilpotent groups if the condition max-*n* or min-*n* is imposed on the groups?

*12. Every group has a unique maximal normal Gruenberg (Baer) subgroup which contains all ascendant Gruenberg (subnormal Baer) subgroups.

13. Prove that a group G is hypercentral if and only if to each countable sequence of elements $g_1, g_2, \ldots$ there corresponds an integer r such that $[g_1, g_2, \ldots, g_r] = 1$.

14. (Černikov). A group-theoretical property $\mathscr{P}$ is said to be of *countable character* if a group has $\mathscr{P}$ whenever all its countable subgroups have $\mathscr{P}$. Prove that nilpotence and hypercentrality are properties of countable character. [*Hint*: Use Exercise 12.2.13.]

15. (Baer). Prove that the normalizer condition is a property of countable character. [*Hint*: Assume that every countable subgroup of G satisfies the normalizer condition but G has a proper subgroup H such that $H = N_G(H)$. Choose a countable subgroup X satisfying $1 < X \cap H < X$. If $x \in X \backslash (X \cap H)$, there is an x^* in H such that $(x^*)^x$ and $(x^*)^{x^{-1}}$ do not both belong to H. Define $X^* = \langle X, x^* | x \in X \rangle$. Now $X_1 = X$ and $X_{i+1} = X_i^*$. Consider the union U of the chain $X_1 \leq X_2 \leq \cdots$.]

*16. If $N \lhd G$ and N is hypercentral, prove that $N' \leq \text{Frat } G$. [*Hint*: Let M be a maximal subgroup of G not containing N. Prove that $N \cap M \lhd G$ and $N/N \cap M$ is a principal factor of G.]

12.3. Engel Elements and Engel Groups

In this and the following sections generalized nilpotent groups which are not locally nilpotent will be considered. Among the best known groups of this sort are the so-called Engel groups. This is a subject whose origins lie outside group theory, in the theory of Lie rings.

Engel Elements

An element g of a group G is called a *right Engel element* if for each x in G there is a positive integer $n = n(g, x)$ such that $[g, {}_n x] = 1$. Notice that the variable element x appears on the *right* here. If n can be chosen independently of x, then g is a *right n-Engel element* of G, or less precisely a *bounded right Engel element*. The sets of right and bounded right Engel elements of G

are written

$$R(G) \quad \text{and} \quad \bar{R}(G).$$

Left Engel elements are defined in a similar fashion. If $g \in G$ and for each x in G there exists an integer $n = n(g, x)$ such that $[x, {}_n g] = 1$, then g is a *left Engel element* of G. Here the variable x is on the left. If n can be chosen independently of x, then g is a *left n-Engel element* or *bounded left Engel element*. Write

$$L(G) \quad \text{and} \quad \bar{L}(G)$$

for the sets of left and bounded left Engel elements of G.

While it is clear that these four subsets are invariant under automorphisms of G, it is unknown if they are always subgroups. What inclusions hold between the four subsets?

12.3.1 (Heineken). *In any group G the inverse of a right Engel element is a left Engel element and the inverse of a right n-Engel element is a left $(n + 1)$-Engel element. Thus*

$$R(G)^{-1} \subseteq L(G) \qquad \textit{and} \qquad \bar{R}(G)^{-1} \subseteq \bar{L}(G).$$

Proof. Let x and g be elements of G. Using the fundamental commutator identities we obtain

$$\begin{aligned} [x, {}_{n+1}g] &= [[x, g], {}_n g] = [[g^{-1}, x]^g, {}_n g] \\ &= [[g^{-1}, x], {}_n g]^g \\ &= [[gg^{-x}, {}_n g]^g \\ &= [g^{-x}, {}_n g]^g. \end{aligned}$$

Hence $[g^{-x}, {}_n g] = 1$ implies that $[x, {}_{n+1} g] = 1$. Both parts of the result now follow. □

It is still an open question whether every right Engel element is a left Engel element.

The two sets of left Engel elements are closely related to the Hirsch–Plotkin radical and the Baer radical respectively, the latter being the unique maximal normal Baer subgroup (which exists in any group—see Exercise 12.2.11). Moreover it turns out that the two sets of right Engel elements have much to do with the hypercenter and the ω-center.

12.3.2. *Let G be any group. Then:*

(i) *$L(G)$ contains the Hirsch–Plotkin radical and $\bar{L}(G)$ the Baer radical;*
(ii) *$R(G)$ contains the hypercenter and $\bar{R}(G)$ contains the ω-center.*

Proof. (i) Let g belong to the Hirsch–Plotkin radical H and let $x \in G$. Then $[g, x] \in H$ and thus $K = \langle g, [x, g] \rangle \leq H$. It follows that K is nilpotent and $[x, {}_n g] = 1$ for some $n > 0$, so that $g \in L(G)$. Next suppose that g belongs to

the Baer radical; then $\langle g \rangle$ is subnormal in G, and there is a series of finite length $\langle g \rangle = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$. Clearly $[x, g] \in G_{n-1}$, $[x, {}_2g] \in G_{n-2}$ for any x in G, and so on; finally $[x, {}_ng] \in G_0 = \langle g \rangle$. Consequently $[x, {}_{n+1}g] = 1$ and $g \in \bar{L}(G)$.

(ii) Let g belong to the hypercenter of G and let $x \in G$. Suppose that $[g, {}_nx] \neq 1$ for all n. Now $g \in \zeta_\alpha G$ for some first ordinal α, which cannot be a limit ordinal; for if it were, $\zeta_\alpha G$ would equal $\bigcup_{\beta<\alpha} \zeta_\beta G$. Hence $g \in (\zeta_\alpha G)\backslash(\zeta_{\alpha-1} G)$. It follows that $[g, x] \in \zeta_{\alpha-1} G$, so that by the same argument $[g, x] \in (\zeta_{\alpha'} G)\backslash(\zeta_{\alpha'-1} G)$ where $\alpha' < \alpha$. Similarly $[g, {}_2x] \in (\zeta_{\alpha''} G)\backslash(\zeta_{\alpha''-1} G)$ where $\alpha'' < \alpha' < \alpha$. Since this process cannot terminate, it leads to an infinite descending chain of ordinals $\cdots < \alpha'' < \alpha' < \alpha$; this cannot exist. Hence $g \in R(G)$. Finally, if $g \in \zeta_n G$ and $x \in G$, then $[g, {}_nx] = 1$ and $g \in \bar{R}(G)$. □

The major goal of Engel theory is to find conditions which will guarantee that $L(G)$, $\bar{L}(G)$, $R(G)$, and $\bar{R}(G)$ are subgroups which coincide with the Hirsch–Plotkin radical, the Baer radical, the hypercenter and the ω-center respectively. That equality does not always hold is shown by a famous example of Golod [a59] (see also [b33]) of a finitely generated infinite p-group G such that $G = L(G) = R(G)$. This group does not equal its Hirsch–Plotkin radical, otherwise it would be finite.

Engel Groups

For any group G the statements $G = L(G)$ and $G = R(G)$ are clearly equivalent, and a group with this property is called an *Engel group*. By 12.3.2 (or directly) we see that every locally nilpotent group is an Engel group. Golod's example mentioned above shows that Engel groups need not be locally nilpotent. Thus Engel groups represent a rather wide generalization of nilpotent groups.

By an *n-Engel group* is meant a group G such that $[x, {}_ny] = 1$ for all $x, y \in G$; that is, every element is both left and right n-Engel. Thus the class of n-Engel groups is the variety determined by the law $[x, {}_ny] = 1$. For example, a nilpotent group of class n is an n-Engel group. On the other hand, n-Engel groups need not be nilpotent—see Exercise 12.3.1. A group is a *bounded Engel group* if it is n-Engel for some n.

Engel Structure in Soluble Groups

The sets $L(G)$ and $\bar{L}(G)$ are well-behaved if G is a soluble group.

12.3.3. (Gruenberg). *Let G be a soluble group.*

(i) *$L(G)$ coincides with the Hirsch–Plotkin radical and is a Gruenberg group. Thus a soluble Engel group is a Gruenberg group.*
(ii) *$\bar{L}(G)$ coincides with the Baer radical. Thus a soluble bounded Engel group is a Baer group.*

Proof. (i) Let $g \in L(G)$: by 12.2.7 it suffices to prove that $\langle g \rangle$ is ascendant in G. Let d be the derived length of G. If $d \leq 1$, then G is abelian and $\langle g \rangle \lhd G$; thus we can assume $d > 1$ and write $A = G^{(d-1)}$. Now obviously $gA \in L(G/A)$, so $\langle g, A \rangle$ is ascendant in G by induction on d. It remains to prove that $\langle g \rangle$ is ascendant in $\langle g, A \rangle$.

Since A is abelian, the mapping $a \mapsto [a, g]$ is an endomorphism ξ of A. If $F \neq 1$ is a finite subset of A, there is an integer n such that $[x, {}_n g] = 1$ for all x in F; hence $F^{\xi^n} = 0$, which clearly implies that $C_A(g) \neq 1$. Now define subgroups $1 = A_0, A_1, \dots$ by the rules $A_{\alpha+1}/A_\alpha = C_{A/A_\alpha}(g)$ and $A_\lambda = \bigcup_{\beta<\lambda} A_\beta$ where α is an ordinal and λ a limit ordinal. Since we can always find a nontrivial element that is centralized by g in a nontrivial quotient of A, there is an ordinal γ such that $A_\gamma = A$. Now $\langle g, A_\alpha \rangle \lhd \langle g, A_{\alpha+1} \rangle$ because g centralizes $A_{\alpha+1}/A_\alpha$. It follows that the $\langle g, A_\alpha \rangle$ form an ascending series from $\langle g \rangle$ to $\langle g, A \rangle$ and $\langle g \rangle$ is ascendant in G.

(ii) Now suppose that g is a left n-Engel element. Keeping the same notation, we have $\langle g, A \rangle$ subnormal in G by induction on d. Here $[a, {}_n g] = 1$ for *all* a in A, so $\langle g, A \rangle$ is nilpotent and $\langle g \rangle$ is subnormal in $\langle g, A \rangle$ and hence in G. Therefore g is in the Baer radical. □

On the other hand, quite simple examples show that $R(G)$ may be larger than the hypercenter even when G is soluble (Exercise 12.3.1).

The following was the first theorem to be proved about Engel groups.

12.3.4 (Zorn). *A finite Engel group is nilpotent.*

Proof. Suppose that this is false and let G be a finite Engel group which has smallest order subject to being nonnilpotent. Then every proper subgroup of G is nilpotent and G is soluble by Schmidt's theorem (9.1.9). By 12.3.3, G equals its Hirsch–Plotkin radical, which means that G is nilpotent since it is finite. □

2-Engel Groups

Obviously a 0-Engel group has order 1 and the 1-Engel groups are exactly the abelian groups. Greater interest attaches to the class of 2-Engel groups; this, it turns out, includes all groups of exponent 3.

12.3.5. *A group of exponent* 3 *is a* 2-*Engel group.*

Proof. Let G be a group of exponent 3 and let $x, y \in G$. Then $(xy^{-1})^2 = (xy^{-1})^{-1} = yx^{-1}$. Post-multiplication by y^2 yields

$$xy^{-1}xy = yx^{-1}y^2 = y^{-2}x^{-1}y^{-1} = y^{-1}(y^{-1}x^{-1}y^{-1}) = y^{-1}x(x^{-1}y^{-1})^2.$$

Therefore

$$x(y^{-1}xy) = y^{-1}x(x^{-1}y^{-1})^{-1} = (y^{-1}xy)x.$$

It follows that x commutes with x^y and hence with $x^{-y}x = [y, x]$. Thus $[y, x, x] = 1$. □

We shall now establish the basic result on 2-Engel groups.

12.3.6 (Levi). *Let G be a 2-Engel group and let x, y, z, t be elements of G. Then*:

(i) x^G *is abelian*;
(ii) $[x, y, z] = [z, x, y]$;
(iii) $[x, y, z]^3 = 1$;
(iv) $[x, y, z, t] = 1$, *so that G is nilpotent of class* ≤ 3.

Proof. (i) We have $[x, x^y] = [x, x[x, y]] = [x, [x, y]]$. Now x commutes with $[y, x]$ and hence with $[x, y]$. Therefore x and x^y commute, and it follows by conjugation that any two conjugates of x commute. Hence x^G is abelian.

(ii) Let $A = x^G$, an abelian group. The mapping $a \mapsto [a, y]$ is an endomorphism of A which will be written y^*. Since $(y^*)^2$ sends a to $[a, y, y] = 1$, we have $(y^*)^2 = 0$.

From the elementary commutator formulae for $[x, yz]$ and $[x, y^{-1}]$ we obtain the results

$$(yz)^* = y^* + z^* + y^*z^* \tag{3}$$

and

$$(y^{-1})^* = -y^*. \tag{4}$$

Now $(yz)^{-1}$ commutes with $[a, yz]$, so by (3) and (4) we have

$$\begin{aligned} 0 = (yz)^*(z^{-1}y^{-1})^* &= (y^* + z^* + y^*z^*)(-z^* - y^* + z^*y^*) \\ &= -y^*z^* - z^*y^*. \end{aligned}$$

Therefore

$$y^*z^* = -z^*y^*, \tag{5}$$

which tells us that $[x, y, z] = [x, z, y]^{-1}$. Since A is abelian, $[x, z, y]^{-1} = [[x, z]^{-1}, y] = [z, x, y]$; hence $[x, y, z] = [z, x, y]$ as required.

(iii) Using (ii) we obtain $[x, y^{-1}, z]^y = [x, y^{-1}, z]$ and thus $[x, y^{-1}, z]^y = [[x, y]^{-1}, z] = [x, y, z]^{-1}$. Now apply the Hall–Witt identity (5.1.5) and (ii) to get the result.

(iv) By (5) we have $y^*(zt)^* + (zt)^*y^* = 0$. Expanding this with the aid of (3) and (5) one obtains

$$\begin{aligned} 0 &= y^*z^* + y^*t^* + y^*z^*t^* + z^*y^* + t^*y^* + z^*t^*y^* \\ &= 2y^*z^*t^*. \end{aligned}$$

Hence $[x, y, z, t]^2 = 1$. But also (iii) implies that $[x, y, z, t]^3 = 1$, so $[x, y, z, t] = 1$. □

Notice that G is a 2-Engel group if and only if x^G is abelian for all x in G. While 3-Engel groups are less well-behaved, it is true that G is 3-Engel if and only if x^G is nilpotent of class ≤ 2 for all x in G (Kappe and Kappe [a111]). In general 3-Engel groups are not nilpotent, but they are always locally nilpotent (Heineken [a87]). For a clear and concise account of the theory of 3-Engel groups see Gupta [b30].

Engel Structure in Groups with the Maximal Condition

According to 12.3.4 a finite Engel group is nilpotent. Can we weaken the hypothesis of finiteness here? Certainly finitely generated will not do—Golod's example tells us that—but is there any hope for the maximal condition? The answer turns out to be affirmative; in fact groups with max have excellent Engel structure.

12.3.7 (Baer). *Let G be a group which satisfies the maximal condition. Then $L(G)$ and $\bar{L}(G)$ coincide with the Hirsch–Plotkin radical, which is nilpotent, and $R(G)$ and $\bar{R}(G)$ coincide with the hypercenter, which equals $\zeta_m G$ for some finite m. In particular, if G is an Engel group, it is nilpotent.*

Most of the labor of the proof resides in establishing the following special case.

12.3.8. *If G satisfies* max *and $a \in L(G)$, then a^G is finitely generated and nilpotent.*

Proof. Assume that the statement is false.

(i) Let $\{a^G\}$ denote the *set* of all conjugates of a in G. A subgroup X of G will be called *a-generated* if it is generated by those conjugates of a that it contains, in symbols $X = \langle X \cap \{a^G\}\rangle$.

(ii) *If X and Y are nilpotent a-generated subgroups such that $X < Y$, then $N_Y(X)$ contains at least one conjugate of a which does not belong to X.*

Because Y is nilpotent, X is subnormal in Y and there is a series $X = X_0 \lhd X_1 \lhd \cdots \lhd X_s = Y$. Since $X \neq Y$ and Y is a-generated, $Y \backslash X$ must contain a conjugate of a. Hence there is an integer i such that

$$X \cap \{a^G\} = X_i \cap \{a^G\} \subsetneqq X_{i+1} \cap \{a^G\}.$$

Suppose that $y \in X_{i+1} \cap \{a^G\}$ and $y \notin X_i$. Then y normalizes X_i, so that $(X \cap \{a^G\})^y = (X_i \cap \{a^G\})^y = X_i \cap \{a^G\} = X \cap \{a^G\}$. Since $X \cap \{a^G\}$ generates X, the element y normalizes X.

(iii) *There exist two distinct maximal a-generated nilpotent subgroups U and V.*

Consider the set $\mathscr{S}$ of all a-generated nilpotent subgroups. By the maximal condition each element of $\mathscr{S}$ is contained in a maximal element. If there

were just one maximal element of $\mathscr{S}$, say M, then it would contain $\langle a \rangle$; for $\langle a \rangle \in \mathscr{S}$. But $M \lhd G$ since conjugates of M belong to $\mathscr{S}$; thus $a^G \leq M$ and a^G is nilpotent, a contradiction.

(iv) Consider the subgroup

$$I = \langle U \cap V \cap \{a^G\} \rangle.$$

Here we can suppose that U and V have been chosen so that I is maximal. Now define

$$W = \langle N_U(I) \cap \{a^G\} \rangle.$$

From its definition we see that I is a-generated and also that $I \neq U$ since $I \leq V$. By (ii) we conclude that $I < W$. For the same reason $N_V(I) \cap \{a^G\}$ has an element v that does not belong to I and hence not to U.

Suppose that $v \in N_G(W)$. Now max shows that W can be finitely generated, say by $a^{g_1}, \dots, a^{g_m}$. Keeping in mind that v is conjugate to a and therefore belongs to $L(G)$, we find an $n > 0$ such that $[a^{g_i}, {}_n v] = 1$ for $i = 1, \dots, m$. Let $H = \langle v, W \rangle$; then clearly $W' \lhd H$ and H/W' is nilpotent of class $\leq n$. But W is nilpotent since U is, so we can apply Hall's criterion (5.2.10), concluding that H is nilpotent. Since W is a-generated and v is conjugate to a, we see that H is a-generated. Therefore $H \in \mathscr{S}$ and H is contained in a maximal element T of $\mathscr{S}$. Now $v \in T \backslash U$, which shows that $T \neq U$. Also $W \leq H \leq T$, so $N_U(I) \cap \{a^G\} \subseteq U \cap T \cap \{a^G\}$ and $I < W \leq \langle U \cap T \cap \{a^G\} \rangle$. But this contradicts the maximality of I.

(v) It follows from the preceding argument that $v \notin N_G(W)$. Since $I < U$, there is an element u in $N_U(I) \cap \{a^G\}$ which is not in I: here we use (ii). Now $[v, {}_n u] = 1$ for some n because $u \in L(G)$. Hence there is a least integer k such that $[v, {}_k u]$ normalizes W; moreover $k > 0$ since $v \notin N_G(W)$. Writing $z = [v, {}_{k-1} u]$, we have $[z, u] = (u^z)^{-1} u \in N_G(W)$ and $u \in W$, whence $u^z \in N_G(W)$. Now we may show just as in (iv) that $K = \langle u^z, W \rangle$ belongs to $\mathscr{S}$, and is therefore contained in a maximal element R of $\mathscr{S}$. But, since W is a-generated, $\langle U \cap R \cap \{a^G\} \rangle \geq W > I$, which will contradict the maximality of I unless $R = U$. Therefore $u^z \in U$.

By construction u and v belong $N_G(I)$, so that $z = [v, {}_{k-1} u] \in N_G(I)$. Since u^z is conjugate to a, we obtain $u^z \in N_U(I) \cap \{a^G\} \subseteq W$, by definition of W. Also $u \in W$, so we have $u^z \in W^z$. It follows that $u^z \in U \cap W^z \cap \{a^G\}$. Now $I \leq W$ and $I = I^z \leq W^z$, so that $I < \langle U \cap W^z \cap \{a^G\} \rangle$. Thus W^z is contained in a maximal element of $\mathscr{S}$ which must equal U; otherwise the maximality of I would again be contradicted. Consequently $W^z \leq U$ and $(N_U(I) \cap \{a^G\})^z$ is contained in $N_G(I)^z \cap U \cap \{a^G\} = N_U(I) \cap \{a^G\}$ because $z \in N_G(I)$. Hence $W^z \leq W$. Since $W^z \neq W$, it follows that $W^z < W$; conjugating by negative powers of z, we obtain $W < W^{z^{-1}} < W^{z^{-2}} < \cdots$, which contradicts max. □

***Proof of* 12.3.7.** Here G is a group with max. If $a \in L(G)$, then a^G is nilpotent by 12.3.8, so that a^G is contained in the Hirsch–Plotkin radical H. More-

over H is finitely generated and nilpotent by max. Hence $L(G) = H$ coincides with the Baer radical and hence with $\bar{L}(G)$ by 12.3.2.

The statement about right Engel elements requires a little more attention. Let $a \in R(G)$; then $a^{-1} \in L(G)$ by 12.3.1 and $(a^{-1})^G = a^G = A$ is nilpotent by 12.3.8. Let $x \in G$. Since A_{ab} is generated by finitely many right Engel elements, $[A, {}_k x] \leq A'$ for some positive integer k. Hence $\langle x, A\rangle/A'$ is nilpotent, which implies that $\langle x, A\rangle$ is nilpotent. Refine the upper central series of A to a G-admissible series whose factors are elementary abelian or free abelian of finite rank. Let B be such a factor; then x acts unipotently on B. By 8.1.10 the action of G on B is unitriangular and in consequence $A \leq \zeta_s G$ for some s.

It follows that $R(G) = \zeta_r G$ for some r in view of max. Finally $\bar{R}(G) = \zeta_r G$ by 12.3.2. □

Exercises 12.3

1. Let G be the standard wreath product of a group of order p and an infinite elementary abelian p-group. Prove that G is a $(p+1)$-Engel group, yet $\zeta G = 1$. Deduce that a 3-Engel group need not be nilpotent (see 12.3.6).

2. If G is a locally finite group, show that $L(G)$ equals the Hirsch–Plotkin radical and that $R(G)$ is a subgroup of $L(G)$. [*Hint*: Use 12.3.4.]

3. Let G be a soluble group with a normal series of finite length whose factors are abelian groups of finite rank with finite torsion-subgroups. Prove that $L(G) = \bar{L}(G)$ and $R(G) = \bar{R}(G)$. Show that these conclusions are not valid for arbitrary soluble groups.

4. A soluble p-group of finite exponent is a bounded Engel group.

5. A group G is a 2-Engel group if and only if the identity $[x, y, z] = [y, z, x]$ holds in G.

6. Let x, y be group elements satisfying $[x, {}_n y] = 1$. Prove that $\langle x\rangle^{\langle y\rangle}$ is finitely generated.

7. (Plotkin). If G is a radical group (see Exercise 12.1.2), prove that $L(G)$ coincides with the Hirsch–Plotkin radical and that $R(G)$ is a subgroup of $L(G)$. [*Hint*: Let $\{G_\alpha\}$ be the upper Hirsch–Plotkin series. If X is a finite subset of $L(G) \cap G_2$, prove that $\langle X\rangle$ is nilpotent, using Exercise 12.3.6.]

12.4. Classes of Groups Defined by General Series

There are numerous interesting classes of generalized soluble and nilpotent groups which are defined by means of a *series of general order type*, a concept which will now be explaind.

Definition. Let G be an Ω-operator group. By a (general) Ω-series of G we shall mean a set $\mathbf{S}$ of subgroups, called the *terms* of $\mathbf{S}$, which is linearly ordered by inclusion and which satisfies the following conditions:

(i) If $1 \neq x \in G$, there are terms of $\mathbf{S}$ which do not contain x and the union of all such terms is a term V_x of $\mathbf{S}$.
(ii) If $1 \neq x \in G$, there are terms of $\mathbf{S}$ which contain x and the intersection of all such terms is a term Λ_x of $\mathbf{S}$.
(iii) $V_x \lhd \Lambda_x$.
(iv) Each term of $\mathbf{S}$ is of the form V_x or Λ_x for some $x \neq 1$ in G.

Thus x belongs to the set $\Lambda_x \backslash V_x$; the corresponding quotient group Λ_x/V_x is a *factor* of $\mathfrak{X}$. Notice that no term of $\mathbf{S}$ can lie strictly between V_x and Λ_x. Hence if $x, y \neq 1$, then either $\Lambda_x \leq V_y$ or $\Lambda_y \leq V_x$.

This enables us to linearly order the factors of $\mathbf{S}$ by the rule that Λ_x/V_x precedes Λ_y/V_y if $\Lambda_x \leq V_y$. The *order-type* of $\mathbf{S}$ is the order-type of the set of all factors of $\mathbf{S}$. It follows easily from the definition that

$$V_x = \bigcup \Lambda_y \qquad \text{and} \qquad \Lambda_x = \bigcap V_y$$

where the union is formed over all factors Λ_y/V_y that precede Λ_x/V_x and the intersection over all factors that succeed Λ_x/V_x. These are completeness properties of the series.

If $\mathbf{S}$ has finite order-type, it is clearly just a series of finite length: the smallest V_x will equal 1 and the largest Λ_x will equal G. If $\mathbf{S}$ has the order-type of an ordinal number β, the series will be *an ascending series.* On the other hand, suppose that the order-type of $\mathbf{S}$ is the reverse of an ordinal number β, that is, the set of ordinals $\alpha < \beta$ *in descending order.* Then $\mathbf{S}$ is a *descending series*; this can be written in the form

$$\cdots \lhd H_2 \lhd H_1 \lhd H_0 = G$$

where $H_{\alpha+1} \lhd H_\alpha$ and $H_\lambda = \bigcap_{\gamma<\lambda} H_\gamma$ with α an ordinal and λ a limit ordinal. Note that $\bigcap_{\alpha<\beta} H_\alpha = 1$.

Composition Series

If $\mathbf{S}$ and $\mathbf{S}^*$ are Ω-series in G and if every term of $\mathbf{S}$ is a term of $\mathbf{S}^*$, then $\mathbf{S}^*$ is said to be a *refinement* of $\mathbf{S}$, in symbols $\mathbf{S} \ll \mathbf{S}^*$. If $1 \neq x \in G$, then, with the obvious notation, $V_x \leq V_x^* \leq \Lambda_x^* \leq \Lambda_x$. An Ω-series which has no refinement other than itself is called an *Ω-composition series.*

When Ω is empty, we speak of a *series* and a *composition series*: when Ω is the group of inner automorphisms, we speak of a *normal series* and a *principal series.*

General composition series have the definite advantage that they exist in any group.

12.4.1. *Every Ω-series can be refined to an Ω-composition series.*

Proof. Let $\mathbf{S}_0$ be a given Ω-series in an Ω-group G. Consider the set $\mathscr{X}$ of all refinements of $\mathbf{S}_0$. The relation $\preccurlyeq$ is clearly a partial ordering of $\mathscr{X}$. Let $\mathscr{C} = \{\mathbf{S}^{(\gamma)} | \gamma \in \Gamma\}$ be a chain in $\mathscr{X}$; we shall construct an upper bound for $\mathscr{C}$ in $\mathscr{X}$.

If $1 \neq x \in G$, define $V_x = \bigcup_\gamma V_x^{(\gamma)}$ and $\Lambda_x = \bigcap_\gamma \Lambda_x^{(\gamma)}$ where, of course, $V_x^{(\gamma)}$ and $\Lambda_x^{(\gamma)}$ are terms of $\mathbf{S}^{(\gamma)}$. Certainly $V_x \lhd \Lambda_x$. In addition $V_x^{(\gamma)} \leq V_x \leq \Lambda_x \leq \Lambda_x^{(\gamma)}$ for each γ in Γ. Hence the set $\mathbf{S} = \{\Lambda_x, V_x | 1 \neq x \in G\}$ is linearly ordered by inclusion. It is clear that $\mathbf{S}$ is a series which is an upper bound for $\mathscr{C}$.

We may now apply Zorn's Lemma to produce a maximal element of $\mathscr{X}$. But this is simply a composition series of G. □

The reader should observe that no analogue of the Jordan–Hölder Theorem exists for general series. For example, $\mathbb{Z}$ has the two composition series $\cdots 8\mathbb{Z} < 4\mathbb{Z} < 2\mathbb{Z} < \mathbb{Z}$ and $\cdots 27\mathbb{Z} < 9\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}$, but these have nonisomorphic factors.

Groups with a Central Series

Suppose that the group G has a *central series* $\mathbf{S}$, that is, each term is normal and each factor Λ_x/V_x is central in G. This represents a generalization of nilpotence since G would be nilpotent if $\mathbf{S}$ were finite. Groups with this property are sometimes called *Z-groups.*

12.4.2. *If G is a locally nilpotent group, then G has a central series.*

Proof. By 12.4.1 there is a principal series in G. The factors of this series are principal factors of G and by 12.1.6 they are central in G. □

Groups with a descending central series are examples of Z-groups—these are sometimes called *hypocentral groups* and are characterized by the fact that their lower central series reaches the identity subgroup when continued transfinitely (Exercise 12.4.1). Among the most commonly encountered hypocentral groups are the *residually nilpotent groups.* Even this class is very extensive, containing groups which might be regarded as highly non-nilpotent, for example, free groups by 6.1.10.

Serial Subgroups

A subgroup which occurs in some series of a group G is called *serial.* This must be regarded as a very broad generalization of subnormality and ascendance. It is quite possible for a serial subgroup to be self-normalizing or to have the whole group as its normal closure (Exercise 12.4.4).

Here we are interested in groups having all their subgroups serial; naturally these include all nilpotent groups. Groups of this type can be characterized in terms of the Frattini properties of their subgroups.

12.4.3. *Every subgroup of a group G is serial if and only if $H' \leq \operatorname{Frat} H$ for all $H \leq G$.*

Proof. Of course, the condition on H is equivalent to the normality of all its maximal subgroups. Suppose that every subgroup of G is serial and let M be maximal in H. There is a series in G which includes M. Intersect the terms of this series with H to get a series in H which also includes M. But M is maximal in H, so M and H must be consecutive terms in the second series and $M \lhd H$.

Conversely, assume that the subgroups of G have the property stated. Let $L \leq G$ and define $\mathscr{K}$ to be the set of all chains of subgroups that are refinements of $1 \leq L \leq G$ and that satisfy all the conditions in the definition of a series except perhaps the normality condition (iii). As in 12.4.1 we use Zorn's Lemma to construct a maximal element **S** of $\mathscr{K}$. If X and Y are consecutive terms of **S**, then X must be maximal in Y by maximality of **S**. Hence $X \lhd Y$ and **S** is a series. Consequently L is serial in G. □

In view of this result and 12.1.5 we have the following interesting property of locally nilpotent groups.

12.4.4. *Every subgroup of a locally nilpotent group is serial.*

On the other hand, it has been shown by Wilson [a223] that local nilpotence is not a consequence of the seriality of all subgroups of a group.

Generalized Soluble Groups

The concept of a series permits the creation of many classes of generalized soluble groups. We mention briefly some of the most important.

A group which possesses a series with abelian factors is called an *SN-group*; this is an immensely wide generalization of solubility. For example, it is known that there are simple *SN*-groups which are not of prime order ([b54]).

Somewhat narrower is the class of *SI-groups*, groups which possess a normal series with abelian factors. We shall shortly see that locally soluble groups are *SI*-groups (12.5.2).

An important subclass of *SI* is the class of groups which have an ascending normal series with abelian factors; these are called *hyperabelian groups*. Being much closer to soluble groups this is a relatively tractable class.

We conclude with a result which illustrates the power of the minimal condition.

12.4.5 (Černikov). *An SN-group G satisfies min if and only if it is a soluble Černikov group.*

Proof. We need only prove that if G satisfies min, it is a soluble Černikov group. Let F denote the unique minimal subgroup with finite index in G (see 5.4.22). Then F may be assumed to be nontrivial. Now G is an SN-group, so it has a series with abelian factors. By min the members of this series are well-ordered by set inclusion: thus G has an ascending series with abelian factors. Because thus conclusion applies equally to G/F, this finite group is soluble.

Since $F \neq 1$, there is a smallest term of the ascending series having nontrivial intersection with F, say G_α; here the ordinal α is not a limit ordinal, so $G_{\alpha-1} \cap F = 1$ and $G_\alpha \cap F \simeq (G_\alpha \cap F)G_{\alpha-1}/G_{\alpha-1}$. Thus $G_\alpha \cap F$ is abelian; it is also ascendant in F and contained in the Hirsch–Plotkin radical H of F by 12.1.4. Now H is hypercentral by 12.2.5, so $1 \neq \zeta H \lhd G$ and F contains a nontrivial normal abelian subgroup A of G. The rest of the proof is just like that of 5.4.23 and is left to the reader as an exercise. □

Exercises 12.4

1. Define the *transfinitely extended lower central series* of a group G by the rules $\gamma_1 G = G$, $\gamma_{\alpha+1} G = [\gamma_\alpha G, G]$ and $\gamma_\lambda G = \bigcap_{\beta<\lambda} \gamma_\beta G$ where α is an ordinal and λ a limit ordinal. Prove that G is residually nilpotent if and only if $\gamma_\omega G = 1$, and G is hypocentral if and only if some $\gamma_\alpha G = 1$.

2. A subgroup is called *descendant* if it is a member of some descending series. Find all the descendant subgroups of D_∞. Show that descendance is not preserved with respect to taking quotient groups.

3. Prove that D_∞ is residually nilpotent.

4. Find a serial subgroup which coincides with its normalizer and whose normal closure is the whole group. [*Hint*: Consider McLain's group $M(\mathbb{Q}, F)$.]

5. If every subgroup of a group G is serial and G satisfies min, prove that G is locally nilpotent.

6. A group G is said to be *residually central* if for each nontrivial element x there is a normal subgroup N such that $N \neq xN \in \zeta(G/N)$. Prove that G is residually central if and only if $x \notin [G, x]$ whenever $1 \neq x \in G$. Show also that Z-groups are residually central. (The converse is false—see [a155].)

7. (Ayoub, Durbin). Let G be a residually central group.
   (a) Show that each minimal normal subgroup is contained in the centre of G.
   (b) If H is the hypercenter, prove that G/H is residually central.
   (c) Prove that a residually central group with min-n is a hypercentral Černikov group.

8. A group is hyperabelian if and only if each nontrivial quotient group has nontrivial Fitting subgroup.

9. By an *SN^*-group* is meant a group which has an ascending series with abelian factors. Show that hyperabelian implies SN^* implies radical. Give an example of a finitely generated SN^*-group that is not hyperabelian. [*Hint*: Let $M = M(\mathbb{Q}_2, F_p)$; this is McLain's group with the ordered set $\mathbb{Q}_2$ of all rationals of the form $m2^n$, $m, n \in \mathbb{Z}$, and $F_p = GF(p)$. The assignments $1 + e_{\lambda\mu} \mapsto 1 + e_{\lambda+1\,\mu+1}$ and $1 + e_{\lambda\mu} \mapsto 1 + e_{2\lambda 2\mu}$ determine automorphisms α and β of M respectively. Consider the group $G = \langle \alpha, \beta \rangle \ltimes M$.]

10. Prove that a group G is an SN^*-group if and only if it has an ascending series whose factors are Gruenberg groups.

11. Assume that G is a group with a normal series (of general order type) whose factors are cyclic. Prove that G' is a Z-group.

*12. Complete the proof of 12.4.5.

13. A nontrivial group which has no proper nontrivial serial subgroups is called *absolutely simple*. Prove that a series is a composition series precisely when all its factors are absolutely simple.

14. A finitely generated simple group is absolutely simple. (*Note*: Nonabsolutely simple groups exist [b54].)

15. An *$\overline{SN}$-group* is a group such that the factors in every composition series are abelian. Prove that a group G is an $\overline{SN}$-group if and only if every image of a serial subgroup of G is an SN-group.

16. An *$\overline{SI}$-group* is a group such that all factors in every principal series are abelian. Prove that a group G is an $\overline{SI}$-group if and only if every quotient group of G is an SI-group.

12.5. Locally Soluble Groups

A group is *locally soluble* if every finitely generated subgroup is soluble. Generally speaking, this type of group is much harder to deal with than locally nilpotent groups, essentially because the finitely generated subgroups need not satisfy max. For example, there is no analogue of the Hirsch–Plotkin Theorem—see [b54], §8.1.

Here is one of the few positive results that have been proved about locally soluble groups.

12.5.1 (Mal'cev, McLain). *If G is a locally soluble group, every principal factor of G is abelian.*

Proof. Obviously it is enough to prove that a minimal normal subgroup N of G is abelian. Suppose that this is false and let a, b be elements of N such that $c = [a, b] \neq 1$. Since $c \in N$, we must have $N = c^G$, so that there are elements $g_1, \dots, g_m$ of G such that $a, b \in \langle c^{g_1}, \dots, c^{g_m} \rangle$. Set $H =$

$\langle a, g_1, \dots, g_m, b \rangle$, a soluble group, and consider $A = c^H$. Since A contains a and b, the element c belongs to A'. Consequently $A' \geq c^H = A$ and $A' = A$. However this means that $A = 1$ because H is soluble. □

12.5.2. *Every locally soluble group G is an SI-group. Thus a simple locally soluble group has prime order.*

Proof. By 12.4.1 the group has a principal series and 12.5.1 shows that the factors are abelian. □

On the other hand, infinite simple *SN*-groups were shown to exist by P. Hall (see [b54], §8.4).

We note another simple application of 12.5.1.

12.5.3. *A locally soluble group with the minimal condition on normal subgroups is hyperabelian.*

In general a locally soluble group with min-*n* is not a Černikov group. Moreover the classes of locally soluble groups and hyperabelian groups are incomparable. For more on these matters consult [b54].

Locally Soluble Groups with the Maximal Condition on Normal Subgroups

12.5.4 (McLain). *Let G be a locally soluble group with the maximal condition on normal subgroups. Then to each integer $p \geq 0$ there corresponds an integer $m = m(p, G)$ such that $G^{(m)} \leq \gamma_{r_p}(\cdots \gamma_{r_2}(\gamma_{r_1}(G)\cdots)$ for every sequence of p positive integers $r_1, r_2, \dots, r_p$.*

Proof. If we define $m(0, G) = 0$, the assertion is vacuously true for $p = 0$. Assume that $m = m(p, G)$ has been properly defined. Now $G/G^{(m+1)}$ is finitely generated because it is a soluble group with max-*n* (see 5.4.21). Hence $G = XG^{(m+1)}$ for a suitable finitely generated subgroup X. Then X is soluble, with derived length d, let us say. Now choose any sequence of $p + 1$ positive integers $r_1, \dots, r_{p+1}$. From $G = XG^{(m+1)}$ it follows via Exercise 5.1.7 that $G = X\gamma_{r_{p+1}}(G^{(m)})$. But $X^{(d)} = 1$, so

$$G^{(d)} \leq X^{(d)}\gamma_{r_{p+1}}(G^{(m)}) \leq \gamma_{r_{p+1}}(\gamma_{r_p}\cdots\gamma_{r_1}(G)\cdots).$$

Finally define $m(p + 1, G)$ to be d. □

Using this lemma an interesting criterion for a locally soluble group with max-*n* to be soluble may be established.

12.5.5 (McLain). *Let G be a locally soluble group with the maximal condition on normal subgroups. Then G is soluble if and only if finitely generated subgroups of G have bounded nilpotent lengths.*

Proof. Only the sufficiency requires any discussion. Assume that every finitely generated subgroup of G has nilpotent length at most l. Just as in the proof of 12.5.4 we have $G = XG^{(m+1)}$ for some finitely generated subgroup X. Since X has nilpotent length $\leq l$, there exist integers $r_1, \dots, r_l$ such that $\gamma_{r_l}(\cdots\gamma_{r_1}(X)\cdots) = 1$. Now by 12.5.4 there is an integer $m = m(l, G)$ such that

$$G^{(m)} \leq \gamma_{r_l}(\cdots\gamma_{r_1}(G)\cdots) \leq \gamma_{r_l}(\cdots\gamma_{r_1}(X)\cdots)G^{(m+1)} = G^{(m+1)}.$$

Hence $L = G^{(m)}$ satisfies $L = L'$. If $L = 1$, then G is soluble. Otherwise by max-n we can choose a normal subgroup M of G which is maximal subject to $M < L$. But then L/M is a principal factor of G and 12.5.1 shows that L/M is abelian, which conflicts with $L = L'$. □

12.5.6 (McLain). *A locally supersoluble G with the maximal condition on normal subgroups is supersoluble.*

Proof. If X is a finitely generated subgroup of G, then X is supersoluble and X' is nilpotent by 5.4.10. Thus X has nilpotent length 2 or less. Now apply 12.5.5 to conclude that G is soluble. By 5.4.21 the group G is finitely generated and hence supersoluble. □

Example. *There is a locally soluble group with* max-n *which is not soluble and not finitely generated.* For each positive integer i we construct a finite soluble group G_i with a unique minimal normal subgroup N_i. To start the construction let G_1 be the symmetric group of degree 3 and N_1 the alternating subgroup. Suppose that G_i has been constructed. If p is a prime not dividing $|G_i|$, there exists a faithful irreducible module N_{i+1} for G_i over $GF(p)$ (Exercise 8.1.4). Define G_{i+1} to be the semidirect product of N_{i+1} and G_i. Then N_{i+1} is the unique minimal normal subgroup of G_{i+1} since it is self-centralizing in G_{i+1}.

Define G to be the union of the chain of groups $G_1 < G_2 < \cdots$. Then G is a locally soluble group and it is also a torsion group. Certainly G is not finitely generated—otherwise $G = G_i$ for some i.

Finally we show that G has max-n. Let $1 \neq N \lhd G$; then $N \cap G_j \neq 1$ for some j. Now $N \cap G_i \lhd G_i$; thus $N_i \leq N$ if $N \cap G_i \neq 1$ since N_i is the unique minimal normal subgroup of G_i. Therefore N contains $\langle N_j, N_{j+1}, \dots \rangle$, which implies that $|G : N|$ is finite. It follows that G cannot contain an infinite ascending chain of normal subgroups. Finally G is not soluble: for if it were, it would be finitely generated.

EXERCISES 12.5

1. The class of locally soluble groups is not closed with respect to forming extensions (see Exercise 12.4.9).

2. A locally soluble group need not contain a nontrivial normal abelian subgroup. (Hence locally soluble does not imply hyperabelian.)

3. Let H and K be normal locally polycyclic subgroups of a group. Then the product $J = HK$ is locally polycyclic. Deduce that every group has a unique maximal normal locally polycyclic subgroup and this contains all ascendant locally polycyclic subgroups. [*Hint*: Imitate the proofs of 12.1.2–12.1.4.]

4. If G is a locally soluble group with max-*n*, some term of the (transfinitely extended) derived series equals 1. (Such groups are called *hypoabelian*.)

5. (McLain). A principal factor of a locally polycyclic group is elementary abelian. Deduce that a locally polycyclic group with min-*n* is a torsion group.

6. (McLain). Let G be a locally polycyclic group with min-*n*. Prove that G is a Černikov group if and only if there is an upper bound for the rank of a principal factor of a finite subgroup. [*Hint*: Let r be this upper bound. Suppose that N is a minimal normal subgroup which is an infinite elementary abelian p-group. Choose a linearly independent subset $\{a_1, a_2, \dots, a_{r+1}\}$ of N and put $A = \langle a_1, \dots, a_{r+1} \rangle$. Find a finite subgroup H containing A such that $L \equiv A^H = a^H$ for all $1 \neq a \in A$. Choose M maximal in L subject to $M \lhd H$ and $a_1 \notin M$, and show that $M \cap A = 1$.]

7. (McLain). A locally supersoluble group with min-*n* is a Černikov group. (*Note*: There exist locally soluble groups with min-*n* which are torsion groups but which are not Černikov groups—see McLain [a140].)

CHAPTER 13

Subnormal Subgroups

Although subnormality is a very natural generalization of normality, it received no attention from group theorists until 1939 when Wielandt's fundamental paper [a215] appeared. However there has been much activity in this field in recent years. For a full account of the subject see [b42].

We shall often write

$$H \text{ sn } G$$

to denote the fact that H is a subnormal subgroup of a group G. The most elementary properties of this relation are outlined in Exercise 3.1.8.

13.1. Joins and Intersections of Subnormal Subgroups

A useful tool in the study of subnormality is the *series of successive normal closures*. If X is a nonempty subset of a group G, a sequence of subgroups $X^{G,i}$, $i = 0, 1, 2, \ldots$, is defined by the rules

$$X^{G,0} = G \qquad \text{and} \qquad X^{G,i+1} = X^{X^{G,i}}.$$

Thus X is contained in every $X^{G,i}$ and

$$\cdots X^{G,2} \lhd X^{G,1} \lhd X^{G,0} = G.$$

Of course, $X^{G,1}$ is just the normal closure X^G. It should be clear to the reader how to extend the series transfinitely—see Exercise 13.1.12.

The significance of this series for subnormality is made apparent by the following result.

13.1.1. *Let H sn G and suppose that $H = H_n \lhd H_{n-1} \lhd \cdots \lhd H_0 = G$ is a finite series from H to G. Then $H^{G,i} \leq H_i$ and hence $H = H^{G,n}$.*

Proof. The assertion is true for $i = 0$. If $H^{G,i} \leq H_i$, then $H^{G,i+1} = H^{H^{G,i}} \leq H_{i+1}^{H_i} = H_{i+1}$ and the result follows by induction on i. □

Consequently, *a subgroup H is subnormal in G if and only if $H = H^{G,n}$ for some $n \leq 0$.* Moreover, if H is subnormal in G, it also follows from 13.1.1 that of all series between H and G the series of successive normal closures is shortest.

The length of this shortest series is called the *subnormal index* or *defect* of H in G. This will be written

$$s(G:H).$$

Obviously $s(G:H)$ equals 0 precisely when $H = G$, while $s(G:H) = 1$ if and only if $H \lhd G$ and $H \neq G$. Another evident fact is this: if H sn K sn G, then H sn G and

$$s(G:H) \leq s(G:K) + s(K:H).$$

In addition, if H sn $K \leq G$ and α is a homomorphism from G, then H^α sn K^α and

$$s(K^\alpha : H^\alpha) \leq s(K:H).$$

As regards the distribution of defects of a group there are basically two situations which can arise.

13.1.2. *If a group G has a subnormal subgroup with positive defect i, it has a subnormal subgroup with defect $i - 1$. Hence either there is an integer $s \geq 0$ such that G has subnormal subgroups with defects $0, 1, \ldots, s$ but none of defect greater than s, or else all nonnegative integers occur as defects of subnormal subgroups of G,*

Proof. If H sn G and $s(G:H) = i > 0$, then $s(G:H^{G,i-1}) = i - 1$. The lemma now follows. □

Some interest attaches to *groups which have bounded defects*; these include, of course, all finite groups and also all nilpotent groups (see the proof of 5.2.4). Further examples will be encountered in 13.3.

There is a useful formula for $H^{G,i}$.

13.1.3. *If $H \leq G$, then $H^{G,i} = H[G, {}_iH]$ for all $i \geq 0$.*

Proof. This is trivial if $i = 0$. Assuming the result for i and using 5.1.6, we argue that

$$H^{G,i+1} = H^{H^{G,i}} = H^{[G,{}_iH]} = H[G, {}_{i+1}H]. \qquad \square$$

This formula gives another proof of the result: if G is a nilpotent group of class c and $H \leq G$, then H sn G and $s(G:H) \leq c$.

Intersections of Subnormal Subgroups

It is easy to see that the intersection of any finite set of subnormal subgroups is itself subnormal. More generally there is the following fact.

13.1.4. *Let $\{H_\lambda | \lambda \in \Lambda\}$ be a set of subnormal subgroups of a group G such that $s(G : H_\lambda) \leq s$ for all λ. Then the intersection I of the H_λ's is subnormal in G and $s(G : I) \leq s$.*

Proof. If $x \in I^{G,s}$, then clearly $x \in H_\lambda^{G,s}$ for all λ in Λ; therefore $x \in H_\lambda$ by 13.1.1, so that $I^{G,s} = I$. □

Nevertheless the intersection of an arbitrary collection of subnormal subgroups may well fail to be subnormal.

Example. Consider the infinite dihedral group $G = \langle x, a | a^x = a^{-1}, x^2 = 1\rangle$ and set $H_i = \langle x, a^{2^i}\rangle$. Then $H_{i+1} \lhd H_i$ since $[a^{2^i}, x] = a^{-2^{i+1}}$. Consequently H_i sn G. However $H_1 \cap H_2 \cap \cdots = \langle x \rangle$, a subgroup that coincides with its normalizer in G. Hence the intersection is not subnormal in G.

Joins of Subnormal Subgroups

An altogether more subtle problem is to determine whether the join of a pair—or more generally of any set—of subnormal subgroups is subnormal. If turns out that two subnormal subgroups may well generate a subgroup that is not subnormal.

The following fact is basic.

13.1.5. *Let H sn G and K sn G, and assume that K normalizes H. Then $J = \langle H, K\rangle$ is subnormal in G and $s(G : J) \leq s(G : H)\, s(G : K)$.*

Proof. In the first place, if $H_i = H^{G,i}$, then $H_i = H[G, {}_iH]$ by 13.1.13. Therefore K normalizes H_i.

Next $H_{i+1} \lhd H_iK$ and K sn H_iK. Therefore $H_{i+1}K$ sn H_iK by the elementary properties of subnormality already mentioned, and indeed $s(H_iK : H_{i+1}K) \leq s(G : K)$. Since $H_0K = G$ and $H_rK = HK = J$ if $r = s(G : H)$, it follows that J sn G and $s(G : J) \leq s(G : H)\, s(G : K)$. □

This result can be used to reformulate the join problem for a pair of subnormal subgroups.

13.1.6. *Let H sn G, K sn G and $J = \langle H, K\rangle$. Then the following statements are equivalent:*

(i) J sn G;
(ii) H^K sn G; and
(iii) $[H, K]$ sn G.

Proof. The implications (i) → (ii) → (iii) are trivial consequences of the relations $[H, K] \lhd H^K \lhd J$. Now suppose that (iii) holds. Since $H^K = H[H, K]$ and H normalizes $[H, K]$, we deduce from 13.1.5 that H^K sn G. Similarly $J = H^K K$ and 13.1.5 implies that J sn G. □

A group is said to have *the subnormal joint property* (SJP) if the join of every pair—and hence of every finite set—of subnormal subgroups is subnormal. Now the set of all subnormal subgroups of a group is a partially ordered subset of the lattice of all subgroups, and it is closed under finite intersections. Hence *a group has the* SJP *exactly when the set of all its subnormal subgroups is a sublattice of the lattice of subgroups.* Some examples of groups with the SJP are given by

13.1.7. *Every group with nilpotent derived subgroup has the subnormal join property. In particular this conclusion applies to metabelian groups.*

To prove this one observes that, in the notation of 13.1.6, the subgroup $[H, K]$ is subnormal in G' because the latter is nilpotent. Hence $[H, K]$ sn G and 13.1.6 gives the result.

The next result is of quite a different character, asserting that if a group is sufficiently finite it has the SJP, whereas in 13.1.7 the hypothesis is a form of commutativity. Indeed it is the interplay between finiteness and commutativity which makes the SJP such an elusive property.

13.1.8 (Robinson). *Let G be a group whose derived subgroup satisfies the maximal condition on subnormal subgroups. Then G has the subnormal join property.*

Proof. Let H sn G, K sn G, and $J = \langle H, K\rangle$. Put $s = s(G : H)$. If $s = 0$, then $H = J = G$ and all is clear; assume therefore that $s > 0$.

Let $\{x_1, x_2, \dots, x_n\}$ be a given finite subset of K and put

$$L = \langle H, H^{x_1}, \dots, H^{x_n}\rangle$$

Since $s(H^G : H^{x_i}\rangle = s - 1$, repeated use of an induction hypothesis on s gives L sn H^G and hence L sn G. Now the equation $h^x = h[h, x]$ implies that $\langle H, H^x\rangle = \langle H, [H, x]\rangle$. Consequently $L = \langle H, M\rangle$ where M is the subgroup generated by $[H, x_1], \dots, [H, x_n]$. Since H normalizes $[H, x_i]$, it normalizes M, from which it follows that $M \lhd L$ and thus M sn G. That M sn G' is an immediate consequence. On the basis of max-s we can find a subgroup M which is maximal of the above type. But M must equal $[H, K]$ since one can always add another $[H, x_i]$ to M. Hence $[H, K]$ sn G, which by 13.1.6 implies that J sn G. □

The following special cases are noteworthy.

13.1.9 (Wielandt). *A group satisfying the maximal condition on subnormal subgroups has the subnormal join property.*

13.1.10 (Wielandt). *In a group G with a (finite) composition series the set of all subnormal subgroups is a complete sublattice of the lattice of subgroups.*

***Proof of* 13.1.10.** Let $J = \langle H_\lambda | \lambda \in \Lambda \rangle$ where H_λ sn G. If Λ_0 is a finite subset of Λ, then $J_{\Lambda_0} = \langle H_\lambda | \lambda \in \Lambda_0 \rangle$ sn G by 13.1.9. Since G satisfies max-*s*, there is a maximal subgroup J_{Λ_0}. But clearly J_{Λ_0} equals J and J sn G. The argument for intersections is similar. □

An Example of a Group Without the Subnormal Join Property

Let $\mathscr{S}$ denote the set of all subsets X of the integers $\mathbb{Z}$ such that X contains all integers less than some integer $l(X)$ and none greater than some $L(X)$ where $l(X) \leq L(X)$. Thus, roughly speaking, $\mathscr{S}$ consists of subsets that contain all large negative integers but no large positive ones. With each X in $\mathscr{S}$ we associate symbols a_X and b_X. Let A and B be elementary abelian 2-groups having as bases the sets $\{a_X | X \in \mathscr{S}\}$ and $\{b_X | X \in \mathscr{S}\}$ respectively. Now form the direct product

$$M = A \times B$$

The next step is to define suitable automorphisms of M. Define a_{X*n} to be $a_{X \cup \{n\}}$ if $n \notin X$ and 1 if $n \in X$: a similar convention applies to the b's. For each integer n, automorphisms u_n and v_n of M act according to the following rules. Firstly u_n acts trivially on B and v_n acts trivially on A; secondly

$$u_n\colon a_X \mapsto a_X b_{X*n},$$

$$v_n\colon b_X \mapsto a_{X*n} b_X.$$

It is easy to see that these are in fact automorphisms of M.

Consider the subgroups of Aut M

$$H = \langle u_n | n \in \mathbb{Z} \rangle \qquad \text{and} \qquad K = \langle v_n | n \in \mathbb{Z} \rangle,$$

and put

$$J = \langle H, K \rangle.$$

Finally form the semidirect product

$$G = J \ltimes M.$$

Concerning the group G we shall prove the following.

13.1.11. *The subgroups H and K are subnormal in G with defect equal to 3, but J is not subnormal in G. Thus G does not have the subnormal join property.*

Proof. The following equations are direct consequences of the definitions:

$$[a_X, u_n] = b_{X*n}, \qquad [b_X, u_n] = 1, \tag{1}$$

and

$$[a_X, v_n] = 1, \qquad [b_X, v_n] = a_{X*n}. \tag{2}$$

It is also easy to check from the definitions that $u_m u_n = u_n u_m$ and $u_n^2 = 1$, relations which show H to be an elementary abelian 2-group; of course K too is of this type.

Now write

$$z_{mn} = [u_m, v_n].$$

Using the Hall–Witt identity (5.1.5)

$$[u_m, v_n^{-1}, a_X]^{v_n}[v_n, a_X^{-1}, u_m]^{a_X}[a_X, u_m^{-1}, v_n]^{u_m} = 1,$$

together with (1) and (2), we obtain

$$[a_X, z_{mn}] = a_{X*m*n};$$

similarly

$$[b_X, z_{mn}] = b_{X*m*n}.$$

By the Hall–Witt identity once again

$$[a_X, z_{mn}^{-1}, u_l]^{z_{mn}}[z_{mn}, u_l^{-1}, a_X]^{u_l}[u_l, a_X^{-1}, z_{mn}]^{a_X} = 1.$$

Evaluating this with the aid of (1) and (2) we deduce that $[a_X, [z_{mn}, u_l]] = 1$, with a corresponding result for b_X. Hence $[z_{mn}, u_l] = 1$ and likewise $[z_{mn}, v_l] = 1$. What these equations show is that z_{mn} belongs to the center of J. Thus $[J', J] = 1$ and J is nilpotent of class 2.

Equations (1) and (2) imply that $[H, A] \leq B$ and $[K, B] \leq A$. If $X \in \mathscr{S}$ and n is the largest integer in X, then, on writing $Y = X \backslash \{n\}$, we have $[a_Y, u_n] = b_{Y*n} = b_X$, which implies that $[H, A] = B$. Similarly $[K, B] = A$.

We are now in a position to calculate the successive normal closures of H and K. In the first place $H^G = (H^M)^K = (H^A)^K$; also $H^A = \langle H, [H, A]\rangle = \langle H, B\rangle$. Therefore $H^G = \langle H^K, B^K\rangle = H^K M$. Hence we have $H^{G,2} = (H^{H^K})^M = H^M$ since H sn J and $s(J : H) \leq 2$. Thus $H^{G,2} = \langle H, B\rangle$. Finally $H^{G,3} = H$ because $[H, B] = 1$. Naturally a similar argument applies to K.

However $J^G = G$ because J^G contains both $H^A = \langle H, B\rangle$ and $K^B = \langle K, A\rangle$. Consequently J is not subnormal in G. □

Joins of Infinitely Many Subnormal Subgroups

If the join of an arbitrary set of subnormal subgroups is always subnormal, the group in question is said to have the *generalized subnormal join property*. This is a much stronger property than the SJP.

EXAMPLE. Let $G_i = \langle x_i, a_i | a_i^{2^i} = 1 = x_i^2, a_i^{x_i} = a_i^{-1} \rangle$ be a dihedral group of order 2^{i+1}; then $H_i = \langle x_i \rangle$ is subnormal in G_i with defect t. Now consider the direct products

$$G = G_1 \times G_2 \times \cdots \qquad \text{and} \qquad H = H_1 \times H_2 \times \cdots .$$

Then obviously H_i sn G and the H_i generate H. If H were subnormal in G and $s(G:H) = r$, it would follow that $s(G_i : H_i) \leq r + 1$ for all i, a contradiction. Thus G does not have the generalized SJP. However G does have the SJP because it is a metabelian group (see 13.1.7).

There is a criterion for a group to have the generalized SJP which provides some insight into the nature of that property.

13.1.12 (Robinson). *A group G has the generalized subnormal join property if and only if the union of every chain of subnormal subgroups is subnormal.*

Proof. The condition stated is surely necessary. Let us assume therefore that it is satisfied in G. The first step is to prove that G has the SJP. To this end let H sn G, K sn G and $J = \langle H, K \rangle$: we shall proceed by induction on $s = s(G:H)$, which can be assumed positive. The elements of K may be well-ordered as $\{x_\alpha | \alpha < \gamma\}$ where γ is some ordinal. For $\beta \leq \gamma$ define $L_\beta = \langle H^{x_\alpha} | \alpha < \beta \rangle$. Then the L_β's form a chain and $L_\gamma = H^K$. Now suppose that J is not subnormal in G; then H^K is not subnormal by 13.1.6 and there is a first ordinal β such that L_β is not subnormal in G. This β cannot be a limit ordinal because if it were, L_β would be the union of a chain of subnormal subgroups and our condition would force L_β to be subnormal. Hence $\beta - 1$ exists and $L_\beta = \langle L_{\beta-1}, H^{x_{\beta-1}} \rangle$. However $s(H^G : H^{x_{\beta-1}}) = s - 1$ and $L_{\beta-1}$ sn H^G, so induction on s gives the contradiction L_β sn G.

Now let $\mathscr{S}$ be a possibly infinite set of subnormal subgroups of G. We need to prove that the join of all the members of $\mathscr{S}$ is subnormal. Since G has the SJP, it is permissible to assume that $\mathscr{S}$ is closed under the formation of finite joins. The given chain condition and Zorn's Lemma can be used to produce a maximal element J of $\mathscr{S}$. If $H \in \mathscr{S}$, then $\langle H, J \rangle \in \mathscr{S}$, whence $H \leq J$. Consequently J is the join of *all* the members of $\mathscr{S}$. But J sn G, so G has the generalized SJP. □

Some classes of groups that have the generalized SJP can be read off from the next result.

13.1.13 (Robinson). Let $N \lhd G$ *and assume that N has the generalized subnormal join property while G/N satisfies the maximal condition on subnormal subgroups. Then G has the generalized subnormal join property.*

Proof. Let $\{H_\alpha | \alpha \in A\}$ be any chain of subnormal subgroups of G and let U denote the union of the chain. By 13.1.12 it is enough to prove that U sn G. Now max-*sn* implies that $UN = H_\alpha N$ for some α in A. Hence $U =$

$U \cap (H_\alpha N) = H_\alpha(U \cap N)$. Obviously $U \cap N$ is the union of the chain $\{H_\alpha \cap N | \alpha \in A\}$ and $H_\alpha \cap N$ sn N. Thus by hypothesis $U \cap N$ sn N and certainly $U \cap N$ sn G. Finally $U \cap N \lhd U$, so it follows from 13.1.5 that U sn G. □

For example, *finitely generated metabelian groups have the generalized* SJP, whereas this is not true of arbitrary metabelian groups, as we saw in the example above. For more classes of groups with the SJP, see [b42].

EXERCISES 13.1

1. Find all subnormal subgroups of the groups S_n, D_n, D_∞.
2. Let H sn G, K sn G and $J = \langle H, K \rangle$. If $s(G : H) \leq 2$, prove that J sn G and $s(G : J) \leq 2\, s(G : K)$.
3. Let H sn G, K sn G and $J = \langle H, K \rangle$. If $HK = KH$, prove that J sn G. If $s(G : H) = r$ and $s(G : K) = s$, show also that $s(G : J) \leq rs(s + 1) \cdots (s + r - 1)$. [*Hint*: Let $H_i = H^{J,i}$ and show that $H_i = H_{i+1}(H_i \cap K)$.]
4. There exists a finitely generated soluble group which does not have the SJP. [*Hint*: In the notation of 13.1.11 let $t \in \operatorname{Aut} M$ be defined by $a_X \mapsto a_{X+1}$, $b_X \mapsto b_{X+1}$ where $X + 1 = \{x + 1 | x \in X\}$. Let $L = \langle J, t \rangle \ltimes M$ and prove that L is finitely generated.]
5. Let $D = \operatorname{Dr}_\lambda G_\lambda$ where $G_\lambda \simeq G$. If D has the generalized SJP, prove that there is an upper bound for subnormal defects in G.
6. Let $H \leq G$ and $X \subseteq G$. Show that for any positive integer i the equation $H^{\langle X \rangle} = H^{S_i}[H, {}_i\langle X \rangle]$ holds where $S_i = 1 \cup X \cup (XX) \cup \cdots \cup (\underbrace{X \cdots X}_{i-1})$. [*Hint*: Use 5.1.6.]
7. If $H \leq G$ and K is a finitely generated subnormal nilpotent subgroup of G, then H^K is generated by *finitely many* conjugates of H in K.
8. Let H sn G, K sn G and assume that $H \lhd J = \langle H, K \rangle$. If H and K belong to a class of groups $\mathfrak{X}$ which is closed with respect to forming normal subgroups and finite normal products, prove that J belongs to $\mathfrak{X}$. Give some applications.
9. Generalize the previous exercise to the case where $J = HK = KH$.
10. (J.E. Roseblade and S.E. Stonehewer). Let $\mathfrak{X}$ be a class of groups which is closed with respect to forming normal subgroups and finite normal products. Assume that H sn G, K sn G and $J = \langle H, K \rangle$. If H and K are finitely generated $\mathfrak{X}$-groups, prove that $J \in \mathfrak{X}$ and J sn G. Apply this with $\mathfrak{X}$ equal to the classes of all groups, nilpotent groups, soluble groups. [*Hint*: Use Exercise 13.1.6 and induction on $s(G : H)$.]
11. (H. Wielandt). Let H sn G, K sn G and $J = \langle H, K \rangle$. Define $\mathscr{S}$ to be the set of all subnormal subgroups L of G such that $H \leq L \leq H^K$. Given that $\mathscr{S}$ satisfies the maximal condition, prove that J sn G. Deduce that J sn G if $[H, K]$ satisfies max-*s*.

12. Show how to extend the series of successive normal closures of a subgroup to transfinite ordinals. Use this to give a criterion for a subgroup to be *descendant*, that is, a term of a descending series.

13.2. Permutability and Subnormality

Recall that subgroup H is said to be *permutable* in a group G if $HK = KH$ whenever $K \leq G$. We shall sometimes write

$$H \text{ per } G$$

to denote this relation.

Of course every normal subgroup is permutable, which might lead one to hope that subnormal subgroups also have this property. However any such hope is soon dispelled. If G is a dihedral group of order 8, it can be generated by two subgroups H and K each of order 2. Now H sn G and K sn G since G is nilpotent. However $|HK| = |H| \cdot |K| = 4$, so that $G \neq HK$, and $HK \neq KH$ by 1.3.13.

One may adopt the opposite point of view, asking whether permutable subgroups are subnormal. Here there is an encouraging answer for finite groups at least, as we shall soon see.

13.2.1 (Ore). *If H is a maximal permutable subgroup of a group G, then $H \lhd G$.*

Proof. Suppose that this is false; then there is a conjugate K of H such that $K \neq H$. Now $HK \leq G$ and clearly HK per G. Therefore $G = HK$ and $K = H^{hk}$ for some $h \in H$, $k \in K$. However this implies that $H = K$. □

This has immediate application to permutable subgroups of finite groups.

13.2.2 (Ore). *If H is a permutable subgroup of a finite group G, then H is subnormal in G.*

Proof. Refine $1 \leq H \leq G$ to a chain $1 = G_0 < G_1 < \cdots < G_n = G$ such that G_i is a maximal proper permutable subgroup of G_{i+1}. By 13.2.1 we have $G_i \lhd G_{i+1}$. Since H appears in the chain, H sn G. □

While in general a permutable subgroup of an infinite group need not be subnormal (Exercise 13.2.3), such subgroups are invariably ascendant. To prove this it is necessary to establish a technical lemma.

13.2.3. *Let $G = HK$ where H per G and $K = \langle k \rangle$ is an infinite cyclic group. Assume that $H \cap K = 1$. Then $H \lhd G$.*

Proof. Let p be any prime. Then $HK^p \leq G$ and

$$|G : HK^p| = |HK : HK^p| = |K : (HK^p) \cap K| = |K : K^p| = p.$$

Write X_p for the core of HK^p in G. Then 1.6.9 shows that $|G : X_p|$ divides $p!$. Because $|G : HK^p| = p$, it follows that HK^p/X_p is a Hall p'-subgroup of G/X_p. Since HX_p/X_p is permutable in the finite group G/X_p, we can apply 13.2.2, concluding that HX_p/X_p is subnormal in G/X_p.

Hence $HX_p/X_p \leq O_{p'}(G/X_p)$ by 9.1.1. Consequently

$$H^G X_p/X_p \leq O_{p'}(G/X_p) \leq HK^p/X_p$$

and $H^G \leq HK^p$. Since X_p is the core of HK^p, it follows that $H^G \leq X_p$ for all p. Let N denote the intersection of the X_p for all p. Now G/N is surely infinite; for it contains subgroups of every prime index. Also $N = N \cap (HK) = H(N \cap K)$; if $N \cap K = 1$, then certainly $H = N \lhd G$, so suppose that $N \cap K \neq 1$. Then $|K : N \cap K|$ is finite, K being infinite cyclic, and hence $|HK : H(N \cap K)|$ is finite. But the latter index equals $|G : N|$, a contradiction. □

13.2.4 (Stonehewer). *In any group G a permutable subgroup is ascendant.*

Proof. Let H per G. We shall construct an ascending series $H = H_0 \lhd H_1 \lhd \cdots H_\rho = H^G$ such that H_α per G and $H_{\alpha+1}/H_\alpha$ is finite cyclic group for all $\alpha < \rho$. From this it will follow that H is ascendant in G.

As a first step we form a partial series of the required type in H^G, that is to say, an ascending series $H = H_0 \lhd H_1 \lhd \cdots H_\rho = U \leq H^G$ where H_α per G and $H_{\alpha+1}/H_\alpha$ is finite cyclic. Suppose that this series cannot be extended, in the sense that there does not exist a permutable subgroup K such that $U \lhd K \leq H^G$ and K/U is a nontrivial finite cyclic subgroup. If $U = H^G$, we are finished, so assume that $U \neq H^G$. Then $U^g \nleq U$ for some g in G; for otherwise $H^G \leq U^G = U$. Thus $U \neq UU^g$. Since U per G, we have $UU^g \leq U\langle g \rangle$, and therefore $UU^g = (UU^g) \cap (U\langle g \rangle) = U\langle g^n \rangle = L$, say, for some positive integer n.

If $|L : U|$ is infinite, so is $|U\langle g \rangle : U|$, which implies that $U \cap \langle g \rangle = 1$. But now 13.2.3 may be applied to give the contradiction $U \lhd U\langle g \rangle$ and $U = U^g$. Hence $|L : U|$ is finite. Taking L modulo the core of U and applying 13.2.2 to the resulting quotient group, we conclude that U sn L. If $U = U^{L,r} < U^{L,r-1} = V$, then V is generated by conjugates of U; also $U \lhd V \leq L \leq H^G$ and obviously V/U is a finite cyclic group. Since V is generated by conjugates of U, it is permutable in G. However this contradicts the non-extendability of the partial ascending series. □

Finally, we consider permutable subgroups of finitely generated groups.

13.2.5 (Stonehewer). *A permutable subgroup of a finitely generated group G is subnormal.*

Proof. Assume that H per G. We consider an infinite cyclic subgroup $K = \langle k \rangle$ such that $H \cap K = 1$. We claim that $H \cap K^g = 1$ for every g in G. Suppose that this is false and $H^{g^{-1}} \cap K \neq 1$; then $k^n \in H^{g^{-1}} \leq H\langle g \rangle$ for some $n > 0$. Now $|H\langle k^n \rangle : H|$ is infinite since $H \cap K = 1$; therefore $|H\langle g \rangle : H|$ is infinite and $H \cap \langle g \rangle = 1$. But 13.2.3 shows that $H^{g^{-1}} = H$ which is contrary to assumption.

Let N be the subgroup generated by all infinite cyclic subgroups K such that $H \cap K = 1$. The argument of the previous paragraph has established that $N \lhd G$. In addition $H \lhd HN$ by 13.2.3. Now clearly HN/N per G/N, and also each element of G/N has some positive power in HN/N, by definition of N. Therefore we may pass to the group G/N, which amounts to assuming that $N = 1$.

It will be sufficient to show that $|H^G : H|$ is finite; for then the core of H will have finite index in H^G and we can deduce from 13.2.2 that H sn H^G and thus H sn G.

Let $G = \langle g_1, g_2, \dots, g_n \rangle$; we shall argue by induction on

$$\sum_{i=1}^{n} |H\langle g_i \rangle : H|.$$

Notice that this is finite because of the assumption $N = 1$. Suppose that $H^{g_i} \leq H$ for all i. Some power of g_i belongs to H, so repeated conjugation by g_i yields $H = H^{g_i^r} \leq H^{g_i} \leq H$ for some r; hence $H = H^{g_i}$ for all i and $H \lhd G$. We may therefore assume that $H^{g_i} \nleq H$ for some i; thus $H < HH^{g_i}$ per G. Since

$$|HH^{g_i}\langle g_j \rangle : HH^{g_i}| \leq |H\langle g_j \rangle : H|$$

for all j, and

$$|HH^{g_i}\langle g_i \rangle : HH^{g_i}| < |HH^{g_i}\langle g_i \rangle : H| = |H\langle g_i \rangle : H|,$$

the induction hypothesis leads to the finiteness of $|(HH^{g_i})^G : HH^{g_i}|$. But $(HH^{g_i})^G = H^G$ and $|HH^{g_i} : H| \leq |H\langle g_i \rangle : H| < \infty$, so $|H^G : H|$ is finite as required. □

To conclude we mention without proof a further connection between subnormality and permutability discovered by J.E. Roseblade [a175] in 1965. Let H sn G, K sn G and assume that the tensor product $H_{ab} \otimes K_{ab}$ is trivial: then $HK = KH$. In particular *a perfect subnormal subgroup permutes with every subnormal subgroup.*

Exercises 13.2

1. (a) If H per G and K per G, then HK per G.
   (b) Permutability is not a transitive relation.
   (c) If H per $K \leq G$ and α is a homomorphism from G, then H^α per K^α.
   (d) If H per $K \leq G$ and $L \leq G$, then $H \cap L$ per $K \cap L$.

2. Let $H \leq G$, $K \leq G$, and $J = \langle H, K \rangle$.
   (a) Prove that $J = HKH$ if and only if $HKH = HKHK$.
   (b) (J.S. Wilson). If H sn G, K sn G and $J = HKH$, prove that $J = HK$.

3. (K. Iwasawa). Let $G = T \ltimes A$ where $T = \langle t \rangle$ is infinite cyclic, A is a group of type p^∞, $p > 2$, and $a^t = a^{1+p}$, $(a \in A)$. Prove that every subgroup of G is permutable but not every subgroup is subnormal. [*Hint*: It is enough to show that any two cyclic subgroups permute.]

4. Let $G = \langle H, K \rangle$ where H and K are finitely generated permutable nilpotent subgroups. Prove that G is nilpotent.

5. Let H per G and $K \leq G$ where $H \cap K = 1$ and K is torsion-free. Prove that $H \lhd HK$ and $H \cap K^g = 1$ for all g in G.

6. A permutable subgroup is normalized by every element of prime order.

7. Let H per G where G can be generated by elements of order at most m. Prove that H sn G and $s(G:H)$ does not exceed the number of prime divisors of m (including multiplicities).

8. A subgroup H of a group G is called *subpermutable* if there is a finite chain of subgroups $H = H_0 \leq H_1 \leq \cdots \leq H_n = G$ with H_i per H_{i+1}. Prove that a finite subpermutable subgroup is always subnormal and conclude that for finite subgroups subpermutability and subnormality are identical properties. [*Hint*: Argue by induction on $|H| + n$ where H is finite and subpermutable and n is the length of the chain from H to G. Introduce the subgroup K generated by all elements of prime order.]

9. Show that a finite ascendant subgroup need not be subpermutable.

10. (Itô). Let $G = AB$ where A and B are abelian subgroups of the group G. Prove that G is metabelian. [*Hint*: Let a, $a_1 \in A$ and b, $b_1 \in B$. Write $b^{a_1} = a_2 b_2$ and $a^{b_1} = b_3 a_3$ where $a_i \in A$, $b_i \in B$. Now show that $[a, b]^{a_1 b_1} = [a, b]^{b_1 a_1}$.]

13.3. The Minimal Condition on Subnormal Subgroups

Most of the finiteness restrictions that pertain to the normal or subnormal subgroups of a group are hard to work with in that it is difficult to relate them to structural properties of the group. The one real exception is min-s, the minimal condition on subnormal subgroups, as this section will show.

Simple Subnormal Subgroups

In discussing groups with min-s one must expect to be faced with minimal subnormal subgroups, i.e., simple subnormal subgroups. Such subgroups are, of course, either of prime order or nonabelian; it is those of the latter type that concern us at present. The next result is basic.

13.3.1 (Wielandt). *Let H sn G, K sn G and assume that $H \cap K = 1$. If H is a nonabelian simple group, then $[H, K] = 1$.*

Proof. Let $J = \langle H, K \rangle$ and $s = s(J : H)$. If $s \leq 1$, then $H \lhd J$ and $[H, K] \lhd H$. If $[H, K] \neq 1$, then $H = [H, K]$, so that $H \leq K^J$ and $K^J = J$; therefore $K = J$ by subnormality of K, which leads to the contradiction $H = H \cap K = 1$. Consequently $[H, K] = 1$.

Assume therefore that $s > 1$, so that $H \neq H^k$ for some k in K. Since $H \cap H^k$ sn H, we must have $H \cap H^k = 1$ by simplicity of H. Now $s(H^k : H) = s - 1$, so induction on s yields $[H, H^k] = 1$. For any h_1, h_2 in H we have, therefore,

$$1 = [h_1, h_2^k] = [h_1, h_2[h_2, k]] = [h_1, [h_2, k]][h_1, h_2]^{[h_2, k]},$$

which implies that $[h_1, h_2] \in [H, K]$ and $H' \leq [H, K]$. But $H = H'$ since H is not abelian, so $H \leq [H, K]$; just as before this leads to $K^J = J$ and $H = 1$. □

13.3.2. *A nonabelian simple subnormal subgroup normalizes every subnormal subgroup.*

Proof. Let H sn G and K sn G where H is simple and nonabelian. Since $H \cap K$ sn H, either $H \cap K = 1$, and therefore $[H, K] = 1$ by 13.3.1, or $H \leq K$. The result is now clear. □

13.3.3. *The join of a set of nonabelian simple subnormal subgroups is the direct product of certain of its members and hence is a completely reducible group without center.*

This follows directly from 3.3.11 and 13.3.2.

13.3.4. *If H sn G and H is a nonabelian simple group, then H^G is a minimal normal subgroup of G and H is a direct factor of H^G. Thus $s(G : H) \leq 2$.*

Proof. By 13.3.3 the group H^G is a direct product of conjugates of H, including H we may suppose. If $1 \neq N \lhd G$ and $N \leq H^G$, then N must contain a conjugate of H by 3.3.12. It follows that $H^G \leq N$ and $N = H^G$. □

The Subnormal Socle

If G is any group, the subgroup generated by all the minimal (i.e., simple) subnormal subgroups is called the *subnormal socle* of G. Should G prove to have no minimal subnormal subgroups, we define the subnormal socle to be 1.

13.3.5. *If G is a group and S is its subnormal socle, then $S = S_0 \times S_1$ where S_0 is the centerless completely reducible radical of G and S_1 is a Baer torsion group.*

Proof. Let S_0 and S_1 be the joins of all the minimal subnormal subgroups of G that are nonabelian and abelian respectively. In the first place S_1 is a Baer group by Exercise 12.2.11. In addition it is generated by elements of finite order, so 12.1.1 shows it to be a torsion group. By 13.3.3 the subgroup S_0 is completely reducible and it has trivial center. On the other hand, any normal completely reducible subgroup with trivial centre is certainly contained in S_0.

Obviously $S = S_0 S_1$ and $S_0 \lhd G$, $S_1 \lhd G$. Furthermore 3.3.12 shows that $S_0 \cap S_1$ is a direct product of nonabelian simple groups; on the other hand, it is also a Baer group. Since simple Baer groups have prime order, $S_0 \cap S_1 = 1$ and $S = S_0 \times S_1$. □

One can tell from the structure of the subnormal socle whether a group has a finite number of minimal subnormal subgroups.

13.3.6. *Let G be a group with subnormal socle S. Then the following statements are equivalent.*

(i) *G has only finitely many minimal subnormal subgroups.*
(ii) *S is the direct product of a finite nilpotent group and finitely many nonabelian simple groups.*
(iii) *S satisfies the minimal condition on subnormal subgroups.*

Proof. (i) → (ii) Write $S = S_0 \times S_1$ using the notation of 13.3.5. Certainly S_0 is the direct product of a finite number of nonabelian simple subnormal subgroups of G. As for S_1, it is surely finitely generated; since it is also a Baer group, it is nilpotent (12.2.8). Finally S_1 is a torsion group, so it is actually finite (5.2.18).

(ii) → (iii) This follows from 3.1.7.

(iii) → (i) By 12.2.9 the group S_1 is nilpotent. Also $(S_1)_{ab}$ is generated by elements of prime order and satisfies min. By the structure of abelian groups with min (4.2.11), or by direct observation, $(S_1)_{ab}$ is finite. Theorem 5.2.6 now implies that S_1 is finite. Hence there are only finitely many abelian minimal subnormal subgroups. On the other hand, a nonabelian minimal subnormal subgroup is a direct factor of S_0 and of these there are only finitely many. □

The Wielandt Subgroup

The *Wielandt subgroup* of a group G,

$$\omega(G),$$

is defined to be the intersection of all normalizers of subnormal subgroups of G. Thus $G = \omega(G)$ if and only if every subnormal subgroup of G is normal. For example, according to 13.3.2 all nonabelian minimal subnormal subgroups are contained in $\omega(G)$. In general $\omega(G)$ may well be trivial—see Exercise 13.3.2—but, as the next result will show, this cannot happen in a nontrivial group satisfying min-s.

13.3.7 (Wielandt). *Let N be a minimal normal subgroup of a group G and suppose that N satisfies the minimal condition on normal subgroups. Then $N \leq \omega(G)$.*

Proof. By min-n there is a minimal normal subgroup N_1 of N and $N = N_1^G$. Applying 3.3.11 we can express N as a direct product of finitely many conjugates of N_1, including N_1 itself. Consequently each normal subgroup of N_1 is actually normal in N, a fact which shows N_1 to be simple. By 3.1.7 the group N satisfies min-s.

Now let H sn G and write $s = s(G:H)$. We shall prove that N normalizes H by induction on s, which can, of course, be assumed greater than 1. Since N is minimal normal in G, either $H^G \cap N = 1$ or $N \leq H^G$. The first possibility leads to $[N, H^G] = 1$ and hence to $N \leq N_G(H)$. Assume therefore that $N \leq H^G$. Now there is a minimal normal subgroup M of H^G contained in N; notice that M itself satisfies min-n because N satisfies min-s. Moreover $s(H^G:H) = s - 1$, so the induction hypothesis tells us that M and all its conjugates normalize H. Hence $N = M^G$ normalizes H. □

In groups with min-s the Wielandt subgroup is larger than one might expect in the following sense.

13.3.8 (Robinson, Roseblade). *If a group G satisfies* min-s, *then $\omega(G)$ has finite index in G.*

Proof. Let R denote the finite residual of G and let H sn G. To prove that $H^R = H$ will be conclusive. Accordingly assume that this is false and let the subnormal subgroup H be chosen minimal subject to $H^R \neq H$. Denote by P the join of all the proper subnormal subgroups of H; then $P^R = P$ by minimality of H. Moreover $P \lhd H$ and clearly H/P must be simple. Since $P \lhd HR$ and HR sn G, the group HR/P inherits the property min-s from G. We may therefore invoke 13.3.6 to conclude that HR/P possesses only finitely many minimal subnormal subgroups. If $x \in R$, then $P \leq H^x$ and H^x/P is a simple, and therefore minimal, subnormal subgroup of HR/P. Consequently the number of conjugates of H in R is finite, or, equivalently, $|R: N_R(H)|$ is finite. However R has no proper subgroups of finite index, so $R = N_R(H)$ and $H = H^R$, a contradiction. □

This has an easy but interesting corollary.

13.3.9. *If the group G satisfies the minimal condition on subnormal subgroups, there is an upper bound for the defects of subnormal subgroups of G.*

Proof. Write $W = \omega(G)$ and let H sn G. Then certainly $H \lhd HW$, while G/W is finite by 13.3.8. Now HW/W is subnormal in the finite group G/W, so certainly $s(G:HW) \leq |G:W| = m$. Hence $s(G:H) \leq m + 1$. □

Characterizing Groups with the Minimal Condition on Subnormal Subgroups

13.3.10 (Robinson). *The following statements about a group G are equivalent.*

(i) *G satisfies the minimal condition on subnormal subgroups.*
(ii) *If H is a proper subnormal subgroup of G, there is at least one but only finitely many subnormal subgroups K which are minimal subject to $H < K$.*
(iii) *Each nontrivial image of G has a nontrivial subnormal socle satisfying the minimal condition on subnormal subgroups.*

Proof. (i) → (ii). Suppose G satisfies min-s but possesses infinitely many subnormal subgroups $K_1, K_2, \ldots$ each of which is minimal subject to properly containing H. Now clearly H sn K_i and minimality shows that $H \lhd K_i$ and K_i/H is simple. Thus if $J = \langle K_1, K_2, \ldots \rangle$, then $H \lhd J$ and each K_i/H is a minimal subnormal subgroup of J/H. Let R denote the finite residual of G. Then G/R is finite and $R \leq \omega(G)$ by 13.3.8. Consequently R normalizes each K_i and hence J: thus $J \lhd JR$. Next JR/R is generated by subnormal subgroups K_iR/R of the finite group G/R. Hence JR/R sn G/R by 13.1.9, and JR sn G. It follows that J sn G, from which we conclude that J/H satisfies min-s. However, according to 13.3.6 the group J/H cannot have infinitely many minimal subnormal subgroups, so we have a contradiction.

(ii) → (iii). Suppose that $G \neq 1$ satisfies (ii). Then taking H to be 1 and applying 13.3.6, we conclude that the subnormal socle of G is nontrivial and satisfies min-s. Since the property (ii) is inherited by images of G, we deduce that (iii) is valid in G.

(iii) → (i). This is the main thrust of the theorem. It will be dealt with in four steps.

(a) We begin by forming the series of successive subnormal socles $\{S_\alpha | \alpha \leq \beta\}$. This is the ascending series defined by the rules $S_0 = 1$ and $S_{\alpha+1}/S_\alpha =$ the subnormal socle of G/S_α, together with the usual completeness condition $S_\lambda = \bigcup_{\alpha<\lambda} S_\alpha$ if λ is a limit ordinal. Notice that (iii) guarantees that $S_\alpha < S_{\alpha+1}$ whenever $S_\alpha \neq G$. Thus $G = S_\beta$ and the series reaches G.

(b) *If $1 \neq N \lhd G$, then $N \cap S_1 \neq 1$.* Certainly there is a first ordinal α such that $N \cap S_\alpha \neq 1$, and α cannot be a limit ordinal by the completeness condition. Hence $N \cap S_{\alpha-1} = 1$ and $N \cap S_\alpha \simeq (N \cap S_\alpha)S_{\alpha-1}/S_{\alpha-1}$. Now

$(N \cap S_\alpha)S_{\alpha-1}/S_{\alpha-1}$ is normal in $S_\alpha/S_{\alpha-1}$ and must satisfy min-*s* since the latter does by hypothesis. Hence $N \cap S_\alpha$ satisfies min-*s* and contains a minimal subnormal subgroup of G. It follows that $N \cap S_1 \neq 1$.

(c) *G satisfies* min-*n*. Suppose that $N_1 > N_2 > \cdots$ is an infinite descending chain of normal subgroups of G, and let $I = N_1 \cap N_2 \cap \cdots$. Then G/I inherits property (iii) from G, so we may pass to G/I; in short assume that $I = 1$. Now $N_1 \cap S_1 \geq N_2 \cap S_1 \geq \cdots$ and of course $N_i \cap S_1 \lhd S_1$. However S_1 satisfies min-*s*, so there is an integer i such that $N_i \cap S_1 = N_{i+1} \cap S_1 =$, etc. Since $I = 1$, it follows that $N_i \cap S_1 = 1$, which, in view of (b), means that $N_i = 1$; but this is false.

(d) *Conclusion.* Since G satisfies min-*n*, it has a unique smallest subgroup R with finite index. It follows from 3.1.8 that R too satisfies min-*n*. If it can be shown that every subnormal subgroup of R is normal, it will follow that R satisfies min-*s*, and hence that G satisfies min-*s*.

We first refine the ascending series $\{S_\alpha | \alpha \leq \beta\}$ to one with simple factors; this can be done on the basis of our knowledge of the structure of $S_{\alpha+1}/S_\alpha$ by inserting additional terms.

Now let H be any subnormal subgroup of R. Intersecting H with the terms of the refined series described in the previous paragraph, one obtains an ascending series of H whose factors, after deletion of repetitions, are all simple. The length of this series shall be termed the *height* of H. If H is not normal in R, we may assume that H has been chosen of minimal height α with this property. It is obvious that α cannot be a limit ordinal, so there exists a subgroup K, normal in H, such that H/K is simple and K has height $\alpha - 1$. Now if L sn K, then L has height $\alpha - 1$ or less and $L \lhd R$ by choice of H. Since R satisfies min-*n*, we conclude that K satisfies min-*s*.

Next $K \lhd R$ and $|G:R|$ is finite, from which it follows that K has only a finite number of conjugates in G. Each such conjugate is normal in R and has min-*s*, so that $M = K^G$ also satisfies min-*s* by 3.1.7. Consider now the subnormal socle T/K of R/K. Since $T \lhd R$, we have $T \cap M \lhd M$, which shows that $T \cap M$ satisfies min-*s*. Furthermore $T/T \cap M \simeq TM/M$ and the latter, being an image of T/K, is generated by minimal subnormal subgroups. Therefore TM/M is contained in the subnormal socle of G/M, in which it is even subnormal. It follows from the hypothesis that TM/M satisfies min-*s*. By 3.1.7 we conclude that T satisfies min-*s* and 13.3.6 implies that R/K has only finitely many minimal subnormal subgroups. However, if $x \in R$, then $K \lhd H^x$ and H^x/K is minimally subnormal in R/K. Finally, we deduce that H has finitely many conjugates in R, so that $H \lhd R$ since R has no proper subgroups of finite index. □

13.3.11 (Wielandt). *A group G has a composition series of finite length if and only if it has only finitely many subnormal subgroups.*

Proof. If G possesses only finitely many subnormal subgroups, it certainly satisfies max-*s* and min-*s*, and therefore has a composition series of finite

length (see 3.1.5). Conversely, let G have such a composition series: then G has min-s and hence property (ii) of 13.3.10. It is now clear that a composition series in G can be formed in only finitely many ways. Every subnormal subgroup appears in some composition series, so the result follows. □

EXERCISES 13.3

1. If G is a group with min-s and l is the composition length of $G/\omega(G)$, prove that no subnormal defect in G exceeds $l + 1$.
2. If $G = D_\infty$, then $\omega(G) = 1$.
3. If G is a torison-free nilpotent group, prove that $\omega(G) = \zeta G$; does this hold for all nilpotent groups? (*Remark*: According to a theorem of Schenkman [a184] $\omega(G) \leq \zeta_2 G$ if G is nilpotent.)
4. Need a group with max-s have bounded defects?
5. Suppose that G has min-s and let R be its finite residual. Prove that G/R' is the largest quotient of G which is a Černikov group. Deduce that R' is perfect and has no proper subgroups of finite index.
6. If G is a group with min-s, the set of subnormal subgroups of G is a complete lattice.
7. (J.E. Roseblade). Let H sn G and K sn G. If H and K have min-s and H has no proper subgroup of finite index, show that $K^H = K$. [*Hint*: Use induction on $s(G:H)$ and choose K minimal subject to $K^H \neq K$.]
8. (D. Robinson, J.E. Roseblade). Let H sn G, K sn G and $J = \langle H, K\rangle$. If H and K have min-s, prove that J sn G and J has min-s.
9. If H is ascendant in G and H satisfies min-s and has no proper subgroup of infinite index, prove that H sn G and $s(G:H) \leq 2$.
10. (D. Robinson). If a group satisfies the minimal condition on subnormal subgroups with defect ≤ 2, prove that it satisfies min-s. [*Hint*: Use 13.3.10.]

13.4. Groups in Which Normality Is a Transitive Relation

We shall be interested in groups G with the following property: $H \lhd K \lhd G$ always implies that $H \lhd G$. Such groups are called *T-groups*, the "T" standing for transitivity of course. Thus, *T-groups are precisely the groups in which every subnormal subgroup is normal*

Several examples of T-groups are at hand. By 3.3.12 *every completely reducible group is a T-group.* Also *a nilpotent group is a T-group if and only if every subgroup is normal*, i.e., it is *a Dedekind group*. The structure of Dede-

kind groups, completely determined in 5.3.7, will be important in the sequel. The smallest finite group that is *not* a T-group is the dihedral group of order 8.

13.4.1. *If G is a T-group and $C = C_G(G')$, then C is the Fitting subgroup G. Moreover C is a Dedekind group.*

Proof. In the first place, since $[C', C] \leq [G', C] = 1$, the group C is certainly nilpotent and $C \leq \text{Fit } G$. Let N be any normal nilpotent subgroup of G and pick an element x of N. Then $\langle x \rangle$ sn $N \lhd G$, so that $\langle x \rangle \lhd G$ by the property T. Now $G/C_G(x)$ is isomorphic with a subgroup of $\text{Aut}\langle x \rangle$ and the latter is abelian (1.5.5). Hence $G' \leq C_G(x)$ and $x \in C$. It follows that $N \leq C$ and thus $C = \text{Fit } G$. Finally, a subgroup of C is subnormal and hence normal in G. Consequently C is a Dedekind group. □

Using this lemma we may easily establish the basic result on soluble T-groups.

13.4.2 (Robinson). *Every soluble T-group is metabelian.*

Proof. Let us suppose that this is false. Then, because the property T is inherited by quotients, we can find a T-group G such that $G'' \equiv G^{(2)}$ is abelian but nontrivial. Now $G'' \leq \text{Fit } G$ and $\text{Fit } G = C_G(G')$ by 13.4.1, from which it follows that $[G'', G'] = 1$ and G' is nilpotent. Hence $G' \leq \text{Fit } G = C_G(G')$ and we reach the contradiction $G'' = 1$. □

Finite Insoluble T-Groups and the Schreier Conjecture

For the most part we shall be interested in soluble T-groups, but for the moment consider a general T-group G. By 13.4.2 a normal soluble subgroup of G is metabelian. Consequently the union of any chain of normal soluble subgroups of G is soluble (and, of course, normal). It follows easily by Zorn's Lemma that G contains a unique maximal normal soluble subgroup, say S. Moreover the group $\bar{G} = G/S$ is semisimple, i.e., it has no nontrivial normal abelian subgroups. Next $\bar{G}/\bar{G}^{(3)}$ is a soluble T-group, so it is metabelian. Hence $\bar{G}''$ is a perfect semisimple T-group. Disclaiming any interest in soluble T-groups for the present, let us replace $\bar{G}''$ by G.

Now suppose that G is in addition finite and let R be the completely reducible radical of G. Then $R = S_1 \times \cdots \times S_r$ where S_i is a finite nonabelian simple group. Clearly $S_i \lhd G$ and $G/C_G(S_i)$ is isomorphic with a subgroup of $\text{Aut } S_i$; moreover the subgroup $S_i C_G(S_i)/C_G(S_i)$ corresponds to $\text{Inn } S_i$ under this isomorphism.

There is a famous conjecture of Schreier to the effect that the outer automorphism group of a finite simple group is soluble. It has been verified on a

case by case basis, using the classification of finite simple groups. Thus, we may state that Out S_i is soluble, whence so is $G/S_iC_G(S_i)$. However G is perfect, so $G = S_iC_G(S_i) = S_i \times C_G(S_i)$. The same procedure can be applied to $C_G(S_i)$, the end result being that $G = S_1 \times S_2 \times \cdots \times S_r$. Thus *a finite perfect semisimple T-group is completely reducible.*

From now on we shall deal exclusively with soluble T-groups.

Power Automorphisms

An automorphism of a group G that leaves every subgroup invariant is called a *power automorphism.* The terminology is a natural one since such an automorphism maps each element to one of its powers. It is clear that the set of power automorphisms of G is a subgroup of Aut G: this will be written

$$\text{Paut } G.$$

Power automorphisms of abelian groups arise in the theory of soluble T-groups in the following way. Suppose that G is a T-group and that A is a normal abelian subgroup of G. Conjugation by an element of G yields a power automorphism of A, so that there is a monomorphism

$$G/C_G(A) \to \text{Paut } A.$$

While much can be said about power automorphisms of abelian groups, we shall record only the bare minimum necessary for the present exposition. (For further information see Exercise 13.4.9.)

13.4.3. *Let α be a power automorphism of an abelian group A.*

(i) *If A contains an element of infinite order, then either α is the identity or $a^\alpha = a^{-1}$ for all a in A.*
(ii) *If A is a p-group of finite exponent, there is a positive integer l such that $a^\alpha = a^l$ for all a in A. If α is nontrivial and has order prime to p, then α is fixed-point-free.*

Proof. (i) Suppose that a is an element of infinite order in A and let b be any element of A. Then there exist integers l, m, n such that $a^\alpha = a^l$, $b^\alpha = b^m$ and $(ab)^\alpha = (ab)^n$. Notice that $l = \pm 1$ here. The homomorphism condition $(ab)^\alpha = a^\alpha b^\alpha$ gives $a^n b^n = a^l b^m$. If $\langle a \rangle \cap \langle b \rangle = 1$, then $a^n = a^l$ and $b^n = b^m$. Since a has infinite order, $l = n$ and $b^\alpha = b^m = b^l$. If, on the other hand, $\langle a \rangle \cap \langle b \rangle \neq 1$, then $a^r = b^s \neq 1$ for some r and s: in this case application of α yields $a^{rl} = b^{sm} = a^{rm}$, which shows that $l = m$ and again $b^\alpha = b^l$.

(ii) By 4.3.5 the group A is a direct product of cyclic p-groups. Let $\langle a \rangle$ be a cyclic direct factor of maximum order and let $\langle b \rangle$ be any cyclic direct factor of a complement of $\langle a \rangle$ in A. Denote the orders of a and b by p^r and p^s respectively. Now $a^\alpha = a^l$, $b^\alpha = b^m$ and $(ab)^\alpha = (ab)^n$ for certain integers l, m,

n. Hence $a^l b^m = a^n b^n$, which implies that $l \equiv n \bmod p^r$ and $m \equiv n \bmod p^s$. Since $s \leq r$, we obtain $l \equiv m \bmod p^s$ and $b^\alpha = b^l$. This proves the first part.

Suppose that $\alpha \neq 1$ is not fixed-point-free; then $l \equiv 1 \bmod p$ and so $l^{p^{e-1}} \equiv 1 \bmod p^e$ where p^e is the exponent of A. Therefore $\alpha^{p^{e-1}} = 1$. □

Structure of Finite Soluble T-Groups

13.4.4 (Gaschütz). *Let G be a finite soluble T-group and write $L = [G', G]$. Then L is the smallest term of the lower central series, L is abelian and G/L is a Dedekind group. Also $|L|$ is odd and is relatively prime to $|G : L|$, so that L has a complement in G.*

Proof. Like G the group $G/\gamma_4 G$ is a T-group, and since it is nilpotent, it is a Dedekind group and thus of class at most 2. Hence $L \equiv \gamma_3 G = \gamma_4 G$. Since $L \leq G'$, we see at once from 13.4.2 that L is abelian. To show that L has odd order we examine the T-group G/L^2. Conjugation in L/L^2 yields power automorphisms; however L/L^2 is an elementary abelian 2-group and such groups have only one power automorphism, the identity automorphism. It follows that L/L^2 is central in G and $L = [L, G] \leq L^2$. Thus $L = L^2$, which shows that $|L|$ is odd.

Let p be a prime dividing $|L|$; it remains to prove that G/L has no elements of order p; for the existence of a complement will then follow from the Schur–Zassenhaus Theorem (9.1.2). Keep in mind that p must be odd. In what follows L_p and $L_{p'}$ denote the Sylow p- and Sylow p'-subgroups of L. Let $M(p)/L$ be the Sylow p-subgroup of G/L and consider the p-group $M(p)/L_{p'}$; this is abelian because it is a Dedekind group of odd order. Write $C(p)$ for $C_G(L_p)$. Then, since $M(p)/L_{p'}$ is abelian and $L_p \leq M(p)$, we have $[L_p, M(p)] \leq L_p \cap L_{p'} = 1$ and $M(p) \leq C(p)$. Therefore $G/C(p)$ is a p'-group; it is also isomorphic with a subgroup of $\text{Paut}(L_p)$. Let $x \in G \backslash C(p)$-note that $C(p) = G$ would imply that $[L, G] = [L_{p'}, G] < L$. By 13.4.3 the element x induces by conjugation in L_p an automorphsim $a \mapsto a^m$ where $m \not\equiv 1 \bmod p$. Also L_p and $L/L_{p'}$ are isomorphic as $\langle x \rangle$-modules, so x must induce in $M(p)/L_{p'}$ a power automorphism $a \mapsto a^n$ where $n \not\equiv 1 \bmod p$. Hence $M(p) = [M(p), x]L_{p'}$. But $M(p)/L$ is contained in the centre of the Dedekind group G/L because p is odd; consequently $[M(p), x] \leq L$ and thus $M(p) = L$, which completes the proof. □

Constructing Finite Soluble T-Groups

Enough information is now at hand for us to be able to construct all finite soluble T-groups.

Let A be a finite abelian group of odd order and let B be a finite Dedekind group whose order is relatively prime to that of A. Furthermore let

there be given a homomorphism $\theta: B \to \operatorname{Paut} A$ with the property that for each prime p dividing $|A|$ there is an element b_p of B such that b_p^θ acts non-trivially on the p-component of A. Now form the semidirect product

$$G(A, B, \theta) = B \ltimes_\theta A.$$

Obviously this is a finite soluble group. To see that it is also a T-group we must establish a lemma.

13.4.5. *Let N be a normal subgroup of a finite group G and assume that the following hold*:

(i) *G/N is a T-group*;
(ii) *H sn N implies that $H \lhd G$*;
(iii) *$|N|$ and $|G : N|$ are relatively prime.*

Then G is a T-group.

Proof. Assume that $H \lhd K \lhd G$; it must be shown that $H \lhd G$. Now $H \cap N$ sn N, so $H \cap N \lhd G$ by (ii). Thus by passing to quotient groups modulo $H \cap N$ we may suppose that $H \cap N = 1$. This implies that $|H|$ and $|N|$ are relatively prime. Let $M = K \cap (HN) = H(K \cap N)$; then $M \lhd G$ since $HN \lhd G$ in view of (i). Also $H \lhd M$. Hence, if π is the set of all prime divisors of $|G : N|$, then H is the unique Hall π-subgroup of M. Therefore H is characteristic in M and normal in G. □

Applying 13.4.5 with $N = A$ we deduce that $G(A, B, \theta)$ is a T-group. Also by 13.4.4 every finite soluble T-group is isomorphic with some $G(A, B, \theta)$. Notice that if $G = G(A, B, \theta)$, then $A = [A, G]$ by the construction, and $A = \gamma_3 G$.

13.4.6. *The group $G(A, B, \theta)$ is a finite soluble T-group. Every finite soluble T-group is isomorphic with some $G(A, B, \theta)$.*

In general a subgroup of a T-group need not be a T-group. For example, A_5 is simple, so it is certainly a T-group; but A_5 has a subgroup isomorphic with A_4, which is not a T-group. However the situation is different for finite *soluble* T-groups.

13.4.7 (Gaschütz). *A subgroup of a finite soluble T-group G is a T-group.*

Proof. Let $L = \gamma_3 G$ and let $H \leq G$. We know from 13.4.4 that $|L|$ and $|G : L|$ are relatively prime, which clearly implies that $|H \cap L|$ and $|H : H \cap L|$ are relatively prime. Also $H/H \cap L \simeq HL/L \leq G/L$, so that $H/H \cap L$, being isomorphic with a subgroup of a Dedekind group, is certainly a T-group. Subgroups of $H \cap L$ are normal in G, and therefore in H. That H is a T-group is now a direct consequence of 13.4.5. □

13.4.8. *A finite group with cyclic Sylow subgroups is a soluble T-group.*

This follows directly from 10.1.10 and 13.4.5.

Finitely Generated Soluble T-Groups

While much is known about infinite soluble T-groups, the situation is more complicated, there being several distinct types of group, some of which defy classification. A detailed account of these groups is given in [a166]. Here we shall be content to describe the finitely generated soluble T-groups: in this case there are no surprises.

13.4.9 (Robinson). *A finitely generated soluble T-group G is either finite or abelian.*

Proof. Assume that G is infinite and not abelian. Let $C = C_G(G')$. Since G' is abelian (by 13.4.2), the finiteness of C would imply that of G' and hence that of $|G : C|$; in short G would be finite. Therefore C is infinite.

Let $x_1, \dots, x_n$ generate G and put $c_{ij} = [x_i, x_j]$. Then $\langle c_{ij} \rangle \lhd G$ by the property T and the commutativity of G'; it follows that G' is generated by the elements c_{ij}, not merely by their conjugates. Hence G' is a finitely generated abelian group and as such it satisfies max; therefore G satisfies max. Now consider C: this is a finitely generated, infinite nilpotent group (see 13.4.1), so it must contain an element of infinite order (5.2.22). However in view of the structure of Dedekind groups this can only mean that C is abelian. Of course $C \neq G$ by hypothesis.

Now let $g \in G \backslash C$. Then g induces a nontrivial power automorphism in C; using 13.4.3 one deduces that $c^g = c^{-1}$ for all c in C. Moreover this is the only nontrivial power automorphism of C. Since $G' \leq C$, we see that C equals its centralizer in G and $|G : C| = 2$. Thus $G = \langle g, C \rangle$ and $g^2 \in C$, so that $g^2 = (g^2)^g = g^{-2}$ and $g^4 = 1$. Next $[C, g] = C^2$, which implies that $\langle g, C^2 \rangle \lhd G$. Similarly $[C^2, g] = C^4$, which leads to $\langle g, C^4 \rangle \lhd \langle g, C^2 \rangle$. Therefore $\langle g, C^4 \rangle \lhd G$, from which it follows that $[C, g] = C^2 \leq \langle g, C^4 \rangle$. Consequently $C^2 = C^2 \cap (\langle g \rangle C^4) \leq \langle g^2, C^4 \rangle$. Thus we arrive at the equation

$$\langle g^2, C^2 \rangle = \langle g^2, C^4 \rangle.$$

Let T denote the torsion subgroup of C and write $\bar{C} = C/T$. Since $g^2 \in T$, the above equation yields $\bar{C}^2 = \bar{C}^4$. But $\bar{C}$ is a free abelian group, being finitely generated and torsion-free. Therefore $\bar{C}$ is trivial and $C = T$ is finite. □

EXERCISES 13.4

1. A group which satisfies min-s and has no proper subgroups of finite index is a T-group.

2. A Baer T-group is a Dedekind group.
3. A hypercentral T-group is soluble, but not necessarily nilpotent. [*Hint*: The locally dihedral 2-group.]
4. A subgroup of an infinite soluble T-group need not be a T-group.
5. If G is a finite T-group, prove that Frat G is abelian.
6. Let A be a group of type 5^∞ and let θ be a primitive fourth root of unity in the ring of 5-adic integers. Define $G = \langle x \rangle \ltimes A$ where x induces in A the automorphism $a \mapsto a^\theta$. Prove that G is a soluble T-group but Frat G is not even nilpotent (cf. Exercise 13.4.5).
7. Using the notation of 13.4.6, find necessary and sufficient conditions for two groups $G(A, B, \theta)$ and $G(\bar{A}, \bar{B}, \bar{\theta})$ to be isomorphic.
8. (T. Peng, D. Robinson). Let G be a finite group. Prove that G is a soluble T-group if and only if every p-subgroup is pronormal in G for all primes p. [*Hint*: Refer to Exercises 10.3.3–10.3.5. To prove sufficiency let G be a minimal counterexample with the pronormality property. If p is the smallest prime dividing $|G|$, then G is p-nilpotent.]
9. Let A be an abelian torsion group.
   (a) If A_p is the p-component of A, show that Paut $A \simeq \mathrm{Cr}_p$ (Paut A_p).
   (b) If A_p has infinite exponent, prove that Paut A_p is isomorphic with the group of units of the ring of p-adic integers. If $1 \neq \alpha \in$ Paut A_p has finite order and $p > 2$, then α is fixed-point-free and $\alpha^{p-1} = 1$. (This together with 13.4.3 completes the description of power automorphism groups of abelian groups.)
10. Let G be a soluble T-group which is a torsion group. Set $L = [G', G]$. Prove that:
    (a) L_2 is a divisible abelian 2-group (which need not be trivial);
    (b) elements of $L_{2'}$ and $G/L_{2'}$ have relatively prime orders.
    [*Hint*: Imitate the proof of 13.4.4 and appeal to Exercise 13.4.9.]
11. (D. Robinson). Let G be a nonabelian soluble T-group such that $C = C_G(G')$ is *not* a torsion group. Show that C is abelian and that $G = \langle t, C \rangle$ where t induces $a \mapsto a^{-1}$ in C, the element t^2 belongs to C and has order 1 or 2, and $\langle t^2, C^2 \rangle = \langle t^2, C^4 \rangle$. Conversely show that a group with this structure is a T-group. [*Hint*: Examime the proof of 13.4.9.]
12. Let G be a nonabelian soluble group all of whose subgroups are T-groups. Prove that G is a torsion group and $L = [G', G]$ contains no involutions. [*Hint*: use Exercise 13.4.11 to show that $C = C_G(G')$ is a torsion group. Then argue that G is a torsion group with the aid of 13.4.9.]

13.5. Automorphism Towers and Complete Groups

The main result of this section is an important property of subnormal subgroups with trivial centralizer in a finite group. A consequence of this is the famous theorem of Wielandt on automorphism towers. The first result is quite elementary.

13.5.1. *Let H be a subnormal subgroup of a finite group G and let π be a set of primes. Write $R = O_\pi(G)$ and define H/M to be the largest π-quotient group of H. Then R normalizes M.*

Proof. Let $r \in R$: then the mapping $x \mapsto [r, x][R, M, M]$ is a homomorphism from M into the π-group $[R, M]/[R, M, M]$, with kernel K say. Thus M/K is a π-group, which implies that M/L is a π-group where L is the core of K in H. It follows that H/L is a π-group, whence $M = L = K$ by maximality of H/M. Consequently $[r, M] \leq [R, M, M]$ and thus $[R, M] = [R, M, M]$. By 13.1.3 this gives $M^T = M^{T,2} =$ etc., where $T = \langle R, M\rangle$. However $M \lhd H$, so $M \operatorname{sn} G$ and thus $M \operatorname{sn} T$. Hence $M = M^T$ and $M^R = M$. □

We are now equipped to prove the main theorem of this section.

13.5.2 (Wielandt). *Let G be a finite group and suppose that H is a subnormal subgroup of G with the property $C_G(H) = 1$. Then there is an upper bound for $|G|$ depending only on $|H|$.*

Proof. (i) We construct a series of characteristic subgroups in H, say $1 = S_0 < S_1 < \cdots < S_t = H$, in the following manner. If H is semisimple, let S_1 be generated by all (nonabelian) simple subnormal subgroups of H. If H is not semisimple, there is a prime p_1 such that $O_{p_1}(H) \neq 1$; in this case define S_1 to be $O_{p_1}(H)$. Similarly S_2/S_1 is generated by all simple subnormal subgroups of H/S_1 if the latter is semisimple: otherwise $S_2/S_1 = O_{p_2}(H/S_1) \neq 1$ for some prime p_2. Continuing in this manner we construct a series of the required type.

There is a corresponding partial series in G, say $1 = R_0 \leq R_1 \leq \cdots \leq R_t$; this means that R_{i+1}/R_i is generated by all the nonabelian simple subnormal subgroups of G/R_i if S_{i+1}/S_i is the corresponding subgroup of H/S_i, while $R_{i+1}/R_i = O_{p_i}(G/R_i)$ if $S_{i+1}/S_i = O_{p_i}(H/S_i)$.

These series are related by the inclusion

$$S_i \leq R_i.$$

This is certainly true if $i = 0$. Suppose that $i > 0$ and $S_{i-1} \leq R_{i-1}$. Then S_i/S_{i-1}, and hence S_iR_{i-1}/R_{i-1}, is either a p_i-group or is generated by simple subnormal subgroups. Now S_iR_{i-1}/R_{i-1} is subnormal in G/R_{i-1} because $H \operatorname{sn} G$. Hence $S_i \leq R_i$ by definition of R_i.

(ii) *It is sufficient to bound $|R_t|$ in terms of $h = |H|$.* For $H = S_t \leq R_t$, so that $C_G(R_t) \leq C_G(H) = 1$ and $C_G(R_t) = 1$. Therefore $|G| = |G : C_G(R_t)| \leq |\operatorname{Aut} R_t|$ and this last cannot exceed $|R_t|!$.

(iii) *There is an integer $m(h, i)$ such that $|R_i| \leq m(h, i)$.* Notice that the theorem will follow once this has been proved: for we may take i to be t and observe that $t \leq |H| = h$.

We can of course define $m(h, 0)$ to be 1, and we assume that $m = m(h, i - 1)$ has been found so that $|R_{i-1}| \leq m$.

Suppose first that H/S_{i-1} is semisimple. In this case R_i normalizes HR_{i-1}/R_{i-1} by 13.3.2. Moreover $C_{R_i}(HR_{i-1}) \leq C_G(H) = 1$, so that $|R_i| \leq |\mathrm{Aut}(HR_{i-1})|$, which does not exceed $(hm)!$. In this case define $m(h, i)$ to be $(hm)!$.

Otherwise S_i/S_{i-1}, and hence R_i/R_{i-1}, is a p_i-group. Let H/N_i be the largest p_i-quotient of H; then HR_{i-1}/N_iR_{i-1} is surely the largest p_i-quotient of HR_{i-1}/R_{i-1}, and we deduce from 13.5.1 that R_i normalizes N_iR_{i-1}. Therefore, on writing C_i for $C_{R_i}(N_iR_{i-1})$, we have $|R_i : C_i| \leq |\mathrm{Aut}(N_iR_{i-1})| \leq (hm)!$.

Let P_i be a Sylow p_i-subgroup of H and let Q_i be a Sylow p_i-subgroup of HC_i containing P_i. Now P_i normalizes N_iR_{i-1} since $P_i \leq H$; hence $C_i^{P_i} = C_i$. Also $P_i \leq Q_i$. Hence P_i normalizes $T_i = C_i \cap Q_i$. Suppose that $T_i \neq 1$. Now P_iT_i is a p_i-group, so it is nilpotent and T_i contains a nontrivial element x in the center of P_iT_i (see 5.2.1). But $x \in C_i \leq C_G(N_i)$ and $H = P_iN_i$, which leads to $x \in C_G(H) = 1$. By this contradiction $T_i = 1$. However T_i is a Sylow p_i-subgroup of C_i and R_i/R_{i-1} is a p_i-group. It follows that $C_i \leq R_{i-1}$ and $|C_i| \leq m$. Finally $|R_i| \leq m((hm)!)$, a number which we take to be our $m(h, i)$. □

The Automorphism Tower of a Group

Suppose that G is a group with trivial center. If $g \in G$, let g^τ denote conjugation in G by g. Then $\tau: G \to \mathrm{Aut}\, G$ is a monomorphism whose image is $\mathrm{Inn}\, G$, the normal subgroup of all inner automorphisms of G. Suppose that α in $\mathrm{Aut}\, G$ centralizes $\mathrm{Inn}\, G$. Then $g^\tau = (g^\tau)^\alpha = (g^\alpha)^\tau$ by 1.5.4. Since τ is a monomorphism, it follows that $g = g^\alpha$ for all g in G, and $\alpha = 1$. Hence

$$C_{\mathrm{Aut}\, G}(\mathrm{Inn}\, G) = 1.$$

In particular $\mathrm{Aut}\, G$ has trivial center and so the same procedure may be applied to $\mathrm{Aut}\, G$. By making suitable identifications we can in this way construct an ascending chain of groups

$$G = G_0 \lhd G_1 \lhd \cdots G_\alpha \lhd G_{\alpha+1} \lhd \cdots$$

with the properties

$$C_{G_{\alpha+1}}(G_\alpha) = 1, \qquad G_{\alpha+1} = \mathrm{Aut}\, G_\alpha,$$

and $G_\lambda = \bigcup_{\beta<\lambda} G_\beta$ for limit ordinals λ. This chain is called the *automorphism tower* of G. A natural question is whether the tower always terminates.

In studying automorphism towers the following simple lemma is useful.

13.5.3. *Let $G = G_0 \lhd G_1 \lhd \cdots G_\alpha \lhd G_{\alpha+1} \lhd \cdots$, $\alpha < \beta$, be an ascending chain of groups such that $C_{G_{\alpha+1}}(G_\alpha) = 1$ for all α. Then $C_{G_\alpha}(G_0) = 1$.*

Proof. If this is false, there is a least ordinal α such that $C = C_{G_\alpha}(G_0) \neq 1$, and α is certainly not a limit ordinal. We argue that $[G_\gamma, C] = 1$ for all $\gamma < \alpha$. Suppose that this is true for all ordinals preceding γ but not for γ.

Then γ is not a limit ordinal and $[G_{\gamma-1}, C] = 1$, so $C = C_{G_\alpha}(G_{\gamma-1})$. Hence C is G_γ-invariant and $[G_\gamma, C] \leq G_{\alpha-1} \cap C = C_{G_{\alpha-1}}(G_0) = 1$ a contradiction. Therefore $C \leq C_{G_\alpha}(G_{\alpha-1}) = 1$, a final contradiction. □

The classical result on the automorphism tower problem can now be proved.

13.5.4 (Wielandt). *The automorphism tower of a finite group with trivial center terminates after finitely many steps.*

Proof. Let $G = G_0 \lhd G_1 \lhd \cdots$ be the automorphism tower of a finite group G. Then $C_{G_{i+1}}(G_i) = 1$ for all i and thus $C_{G_i}(G_0) = 1$ for all i by 13.5.3. Now G_0 sn G_i; thus 13.5.2 shows $|G_i|$ to be bounded above by a number depending only on $|G|$. Hence there is an integer i such that $G_i = G_{i+1} =$ etc. □

More generally, 13.5.4 is still true if G is a Černikov group (Rae and Roseblade [a161]). On the other hand, there are groups with infinite automorphism tower, the infinite dihedral group being an example (Exercise 13.5.4).

Recently S. Thomas has established the interesting fact that the automorphism tower of any centerless group terminates after a possibly infinite number of steps. The proof is remarkably simple, using only some basic properties of cardinal numbers. In what follows c^+ denotes the successor cardinal to a cardinal number c.

13.5.5. *Let G be an infinite group with trivial center. If $\{G_\alpha\}$ is the automorphism tower of G, then $G_\lambda = G_{\lambda+1} =$ etc., where λ is the smallest ordinal with cardinal $(2^{|G|})^+$.*

Proof. As usual we write the automorphism tower as

$$G = G_0 \lhd G_1 \lhd \cdots G_\alpha \lhd G_{\alpha+1} \lhd \cdots.$$

Then $C_{G_\alpha}(G) = 1$ for all α, by 13.5.3. Let $\varphi \in N_{G_\alpha}(G)$; then the restriction $\varphi_1 = \varphi|_G$ is an element of Aut $G = G_1$, and $\varphi\varphi_1^{-1} \in C_{G_\alpha}(G) = 1$. Therefore $\varphi = \varphi_1$ and we have shown that $N_{G_\alpha}(G) = G_1$ for all α. It follows that $|G_{\alpha+1} : G_1|$ equals the cardinality of the set of conjugates of G in $G_{\alpha+1}$. All such conjugates are contained in G_α, so $|G_{\alpha+1} : G_1| \leq |G_\alpha|^{|G|}$. It follows that

$$|G_{\alpha+1}| = |G_1| \cdot |G_{\alpha+1} : G_1| \leq |G_1| \cdot |G_\alpha|^{|G|} = |G_\alpha|^{|G|}.$$

Let $\alpha < \lambda$ where λ is the smallest ordinal with cardinality $c = (2^{|G|})^+$; thus λ is a limit ordinal. We argue by transfinite induction that $|G_\alpha| < c$ if $\alpha < \lambda$. Assume that $|G_\beta| < c$ for all $\beta < \alpha$. If $\alpha > 0$ is not a limit ordinal, then $|G_\alpha| \leq |G_{\alpha-1}|^{|G|} \leq 2^{|G|} < c$. If, on the other hand, α is a limit ordinal, then $|G_\alpha| \leq 2^{|G|}|\alpha| < c$ since $|\alpha| < c$.

Assume that $G_\lambda \neq G_{\lambda+1}$; then $G_\alpha \neq G_{\alpha+1}$ for $\alpha < \lambda$ and thus $|G_\lambda| \geq c$. Let $\varphi \in G_{\lambda+1} \backslash G_\lambda$ and let $\alpha_1 < \lambda$. We shall argue that there is an ordinal α such that $\alpha_1 \leq \alpha < \lambda$ and $G_\alpha^\varphi = G_\alpha$. In the first place, $|G_{\alpha_1}^{\langle\varphi\rangle}| \leq |G_{\alpha_1}|^{\aleph_0} \leq 2^{|G|} < c$. Now c is a regular cardinal, i.e., it cannot be expressed as a sum of fewer than c smaller cardinals. From this it follows that $G_{\alpha_1}^{\langle\varphi\rangle} \leq G_{\alpha_2}$ for some $\alpha_2 < \lambda$. Similarly $G_{\alpha_2}^{\langle\varphi\rangle} \leq G_{\alpha_3}$ with $\alpha_3 < \lambda$, and so on. Put $\alpha = \lim(\alpha_i)$; then $\alpha < \lambda$ since $|G_\alpha| < c$, and clearly $G_\alpha^\varphi = G_\alpha$.

The argument just given shows that there is an unbounded set A of ordinals preceding λ such that $G_\alpha^\varphi = G_\alpha$ for all α in A. For each α in A we know therefore that $\varphi|_{G_\alpha}$ is an automorphism of G_α, and hence is conjugation by some $g_\alpha \in G_{\alpha+1}$. If β is another ordinal in A and $\alpha \leq \beta$, say, then $g_\alpha g_\beta^{-1} \in C_{G_\lambda}(G_\alpha) \leq C_{G_\lambda}(G) = 1$. Hence $g_\alpha = g_\beta = g$, say, which is independent of α. This means that for every α in A, the automorphism $\varphi|_{G_\alpha}$ is conjugation by g. But C is unbounded, so it follows that φ is conjugation by g in G_λ, and $\varphi \in \text{Inn}\, G_\lambda = G_\lambda$, a contradiction. □

Complete Groups

A group G is said to be *complete* if its center and outer automorphism group are both trivial. This is equivalent to requiring that the conjugation map $G \to \text{Aut}\, G$ be an isomorphism. It is clear that the automorphism tower of a centerless group terminates as soon as a complete group is reached in the tower.

The following result is an immediate consequence of Wielandt's theorem on the automorphism tower.

13.5.6. *A finite group with trivial center is isomorphic with a subnormal subgroup of some finite complete group.*

This certainly indicates that complete groups can have very complex subnormal structure. It is natural to ask if the restriction on the center is necessary here. As it turns out, the theorem remains true when the center is allowed to be nontrivial.

13.5.7. *Every finite group is isomorphic with a subnormal subgroup of some finite complete group.*

Proof. In the light of 13.5.6 we recognize that it suffices to prove the following proposition: *a finite group G is isomorphic with a subnormal subgroup of some finite group with trivial center.*

Let C be the center of G, which we can assume nontrivial. Let p be a prime not dividing $|C|$ and consider the standard wreath product

$$W = G \wr T$$

where $T = \langle t \rangle$ has order p. Identify G with one of the direct factors of the base group B, say G_1. Then G sn W.

It will be necessary to identify the center of W. Suppose that $\zeta W \not\leq B$; then $W = (\zeta W)B$ since $|W : B| = p$, and thus $tb \in \zeta W$ for some $b \in B$. Let $1 \neq a \in G$ and put $c = (a, 1, 1, \dots, 1) \in B$. Then $c^{tb} = (1, a, 1, \dots, 1)^b = c$, which gives the contradiction $a = 1$. Thus $\zeta W \leq B$. If $(g_0, g_1, \dots, g_{p-1}) \in \zeta W$, then, since

$$(g_0, g_1, \dots, g_{p-1})^t = (g_{p-1}, g_0, g_1, \dots, g_{p-2}),$$

it follows that $g_0 = g_1 = \cdots = g_{p-1} = g$ say. Also conjugation by $(x, 1, 1, \dots, 1)$ show that $g^x = g$ for all x in G, so $g \in C$. These considerations demonstrate that ζW consists of those elements of B having all their components equal and in C. Notice that $G_1 \cap (\zeta W) = 1$ and $G_1 \simeq G_1(\zeta W)/\zeta W$ sn $W/\zeta W$. To complete the proof let us show that $G^* = W/\zeta W$ has trivial centre.

Suppose that $u(\zeta W) \in \zeta G^*$ but $u \notin \zeta W$. If $u \notin B$, then $W = \langle u, B \rangle$ and $t \equiv u^m \bmod B$ for some integer m. Choose $1 \neq c \in C$ and take b to be the element $(c, 1, \dots, 1)$. Since $[b, B] = 1$, it follows that $[b, t] = [b, u^m] \in \zeta W$. Now a simple calculation shows that $[b, t] = (c^{-1}, c, 1, \dots, 1)$. Our description of ζW forces p to be 2 and $c^{-1} = c$, so $c^2 = 1$: however $|C|$ is odd since $p \nmid |C|$, so $c = 1$. By this contradiction, $u \in B$.

Let $u = (u_0, u_1, \dots, u_{p-1})$ where $u_i \in G$. If $b = (b_0, b_1, \dots, b_{p-1})$ is an element of B, then $[b, u]$ has components $[b_i, u_i]$, $i = 0, 1, \dots, p - 1$. Take $b_1 = \cdots = b_{p-1} = 1$; since $[b, u] \in \zeta W$, we deduce that $[b_0, u_0] = 1$ for all b_0 in G; hence $u_0 \in C$ and similarly $u_1, \dots, u_{p-1}$ belong to C. Next the ith component of $[u, t]$ is $u_i^{-1}u_{i-1}$ and $[u, t] \in \zeta W$. Hence $y = u_i^{-1}u_{i-1}$ is independent of i and belongs to C. With $u_p = u_0$, the product of the $u_i^{-1}u_{i-1}$ for $i = 1, 2, \dots, p$ equals 1; therefore $y^p = 1$. But C has no element of order p; it follows that $y = 1$. Hence $u_i = u_{i-1}$ for all i and $u \in \zeta W$. □

More on Complete Groups

The chapter concludes with some criteria for a group to be complete, the most famous being the direct factor property.

13.5.8 (Hölder, Baer). *A group G is complete if and only if, whenever $G \simeq N$ and $N \lhd H$, it follows invariably that N is a direct factor of H.*

Proof. (i) Let G be complete and assume that $G \simeq N \lhd H$. If we write C for $C_H(N)$, then $C \lhd H$ and $C \cap N = \zeta N = 1$. Thus $\langle C, N \rangle = C \times N$. Conjuga-

tion in N by an element x of H produces an automorphism which is necessarily inner, induced by $y \in N$ say. Thus $a^x = a^y$ for all a in N and $xy^{-1} \in C$. Therefore $x \in CN$ and $H = C \times N$.

(ii) Conversely, assume that G has the stated property. Suppose that $A = \zeta G$ is nontrivial. By Exercise 5.2.2 there is a finite nilpotent group L such that $L' = \zeta L \simeq A$. Form the central product M of L and G, the subgroups ζL and A being identified by means of the above isomorphism (see 5.3). Thus $M = LG$, $[L, G] = 1$ and $L \cap G = A$. By hypothesis $M = G \times K$ for some K, and $K \leq C_M(G)$. Now $C_M(G) \geq L$, so that $C_M(G) = C_M(G) \cap (LG) = L(\zeta G) = L$. Thus $K \leq L$ and $L = L \cap (GK) = AK$. It follows that $L' = K'$ and $A = \zeta L = L' = K' \leq G \cap K = 1$, a contradiction which shows that $\zeta G = 1$.

Finally, $G \simeq \text{Inn } G \lhd \text{Aut } G$, so by hypothesis $\text{Aut } G = \text{Inn } G \times R$ for some R. But $R \leq C_{\text{Aut } G}(\text{Inn } G)$ and this centralizer consists of the central automorphisms. Since $\zeta G = 1$, such automorphisms are trivial and it follows that $R = 1$ and $\text{Aut } G = \text{Inn } G$. Hence G is complete. □

13.5.9 (Burnside). *If G is a group with trivial centre and* Inn G *is characteristic in* Aut G, *then* Aut G *is complete.*

Proof. Let $A \lhd B$ and let $\psi\colon \text{Aut } G \to A$ be an isomorphism; write $I = (\text{Inn } G)^\psi$. Then I is characteristic in A and therefore normal in B. Thus an element b of B induces an automorphism in I by conjugation. Since $G \simeq \text{Inn } G \simeq I$, the element b also induces an automorphism α in G. To describe α we introduce the conjugation homomorphism $\tau\colon G \to \text{Inn } G$, which is a monomorphism in this case. Then α is given by the rule

$$(g^\alpha)^{\tau\psi} = b^{-1}(g^{\tau\psi})b, \qquad (g \in G).$$

Applying ψ to the equation $\alpha^{-1}g^\tau\alpha = (g^\alpha)^\tau$, we get $(\alpha^\psi)^{-1}g^{\tau\psi}\alpha^\psi = (g^\alpha)^{\tau\psi} = b^{-1}(g^{\tau\psi})b$. Therefore $\alpha^\psi b^{-1} \in C_B(I) = C$, say, and $B = CA$. Also $C \cap A = C_A(I) = 1$ because $C_{\text{Aut } G}(\text{Inn } G) = 1$. Thus $B = C \times A$ and the completeness of Aut G follows via 13.5.8. □

This theorem supplies explicit examples of complete groups.

13.5.10 (Burnside). *If G is a nonabelian simple group, then* Aut G *is complete.*

Proof. Since $G \simeq \text{Inn } G = I$, the subgroup I is minimal normal in $A = \text{Aut } G$. If Aut G is not complete, then on account of 13.5.9 the subgroup I cannot be characteristic in A. Thus $I \neq I^\alpha$ for some α in Aut A. Remembering that I is simple, we have $I \cap I^\alpha = 1$ and thus $[I, I^\alpha] = 1$. Hence $I^\alpha \leq C_A(I) = 1$ and $G = 1$, a contradiction. □

It is a theorem of Hölder that $\text{Aut } A_n \simeq S_n$ provided that $n \neq 2$, 3 or 6. (For the case $n = 5$ see Exercise 1.6.18.) It follows via 13.5.9 (and a special

argument when $n = 3$ or 4) that S_n *is complete if* $n \neq 2$ *or* 6. Of course S_2 is not complete: nor is S_6 and in fact $|\text{Out } S_6| = 2$. For more on these matters see [b40]. It should be mentioned that many finite simple groups are complete.

For comparison with 13.5.10 we mention a result due to Dyer and Formanek [a43]: if F is a noncyclic free group, then Aut F is complete. An account of recent work on complete groups can be found in [a172].

Exercises 13.5

1. Prove that S_3 and S_4 are complete.

2. Prove that the holomorph of $\mathbb{Z}_n$ is complete if and only if n is odd.

3. If A is the additive group of rational numbers of the form $m2^n$, m, $n \in \mathbb{Z}$, show that the holomorph of A is complete.

4. Let $G = D_\infty$; prove that the automorphism tower of G terminates after $\omega + 1$ steps with the group of Exercise 13.5.3.

5. If G is a completely reducible group with trivial centre, show that Aut G is complete.

6. If a complete group G is isomorphic with the derived subgroup of some group, prove that G must be perfect.

7. Let G be a finite group.
   (a) If G is a direct product of (directly) indecomposable complete groups which are pairwise nonisomorphic, then G is complete.
   (b) If G is complete, it has a unique direct decomposition of this type.

8. A finite soluble group is isomorphic with a subnormal subgroup of a complete finite soluble group. [*Hint*: Imitate the proof of 13.5.6 and 13.5.7.]

9. (D. Robinson). An infinite supersoluble group cannot be complete. [*Hint*: Suppose that G is such a group and let A be a maximal normal abelian subgroup of G. First of all show that $C_G(A) = A$. Argue that A contains no involutions and there is a nontrivial element cA^2 in $\zeta(G/A^2) \cap A/A^2$. Write $[g, c] = a(g)^2$ where $a(g) \in A$ and consider the mapping $g \mapsto ga(g)$.]

10. Let G be an arbitrary group.
    (a) Prove that G wr $\mathbb{Z}$ has trivial centre.
    (b) Deduce from (a) and 13.5.5 that G is isomorphic with an ascendant subgroup of a complete group G^*, where $|G^*| \leq (2^{|G|})^+$ if G is infinite.

CHAPTER 14

Finiteness Properties

A *finiteness condition* or *property* is a group-theoretical property which is possessed by all finite groups: thus it is a generalization of finiteness. This embraces an immensely wide collection of properties, numerous examples of which we have already encountered, for example, finiteness, finitely generated, the maximal condition and so on. Our purpose here is to single out for special study some of the more significant finiteness properties.

14.1. Finitely Generated Groups and Finitely Presented Groups

The property of being finitely generated is one that has arisen from time to time. We have seen enough to appreciate that this is a relatively weak finiteness condition which guarantees little else but countability. Indeed the complexity of the structure of finitely generated groups is underscored by the theorem of Higman, Neumann, and Neumann that every countable group can be embedded in a 2-generator group (6.4.7).

Another measure of the vastness of the class of finitely generated groups is the following theorem of B.H. Neumann: *there exist* $2^{\aleph_0}$ *nonisomorphic 2-generator groups.* Thus the set of isomorphism classes of 2-generator groups has the largest cardinality one could expect: for to construct a finitely generated group one has to form a normal subgroup of a free group of finite rank, which can surely be done in at most $2^{\aleph_0}$ ways.

Actually we shall prove a stronger result indicating that even finitely generated soluble groups are very numerous and can have complex structure.

14.1.1 (P. Hall). *If A is any nontrivial countable abelian group, there exist $2^{\aleph_0}$ nonisomorphic 2-generator groups G such that $[G'', G] = 1$, $\zeta G \simeq A$, and $G/\zeta G$ has trivial center.*

Proof. To begin the construction, form the free nilpotent group Y of class 2 on the set $\{y_i | i = 0, \pm 1, \pm 2, \dots\}$. Thus $Y \simeq F/\gamma_3 F$ where F is a free group of countably infinite rank. Now $Y' \simeq F'/\gamma_3 F$, so Y' is a free abelian group with the set of elements $[y_i, y_j] = c_{ij}$, $i < j$ as a basis (see Exercise 6.1.14).

We impose further relations on Y by identifying generators c_{ij} and $c_{i+k\, j+k}$ for all i, j, k. This amounts to forming a quotient group $X = Y/K$ where K is generated by all $c_{ij}^{-1} c_{i+k\, j+k}$: observe that $K \lhd Y$ since $K \leq \zeta Y$. Writing x_i for $y_i K$, we have $\{x_i | i = 0, \pm 1, \dots\}$ as a set of generators of X subject to relations

$$[x_i, x_j, x_k] = 1 \qquad \text{and} \qquad [x_{i+k}, x_{j+k}] = [x_i, x_j]. \tag{1}$$

Clearly Y'/K is torsion-free, so that X is a torsion-free nilpotent group of class 2. Moreover the element

$$d_r = [x_i, x_{i+r}], \qquad (i = 1, 2, \dots),$$

is independent of i and $d_1, d_2, \dots$ form a basis of the free abelian group X'.

The mapping $x_i \mapsto x_{i+1}$ preserves the set of relations (1). Hence by Exercise 2.2.9 there is an automorphism α of X such that $x_i^\alpha = x_{i+1}$. Clearly α has infinite order. Now form the semidirect product

$$H = T \ltimes X$$

where $T = \langle t \rangle$ is infinite cyclic and t operators on X like α. Then

$$d_r^t = [x_0, x_r]^t = [x_1, x_{r+1}] = d_r,$$

so that $X' \leq \zeta H$. Since H/X' is surely metabelian, $H'' \leq X'$ and thus $[H'', H] = 1$. Moreover $H = \langle t, x_0 \rangle$ since $x_i^t = x_{i+1}$.

Let us consider the group $\bar{H} = H/X'$. In this group all commutators in the x_i have been suppressed, which means that, if we write $\bar{t}$ for tX' and $\bar{x}_t$ for $x_i X'$, the elements $\bar{t}$ and $\bar{x}_0$ will generate $\bar{H}$ subject only to the relations $[\bar{x}_i, \bar{x}_j] = 1$, $\bar{x}_i^{\bar{t}} = \bar{x}_{i+1}$. Thus $\bar{H}$ is the standard wreath product of a pair of infinite cyclic groups. By Exercise 1.6.14 the center of $\bar{H}$ is trivial: therefore $\zeta H = X'$.

Since X' is a free abelian group of countably infinite rank while A is countable and abelian, $A \simeq X'/M$ for some $M \leq X'$; here we are using 2.3.7. Now M is contained in the center, so it is normal in H. Thus we can define

$$G_M = H/M.$$

Certainly $[G_M'', G_M] = 1$ and G_M is a 2-generator group. Also $\zeta(G_M) \leq X'/M$ because H/X' has trivial center. It follows that $\zeta(G_M) = X'/M \simeq A$.

All that remains to be done is to show that $2^{\aleph_0}$ nonisomorphic groups can be obtained by varying M within X', always subject to $X'/M \simeq A$ of course. In the first place there are surely $2^{\aleph_0}$ of the M's available. Suppose however that the resulting G_M's fall into countably many isomorphism classes. Then for some M there exist uncountably many isomorphisms $\theta_\lambda: G_{M_\lambda} \to G_M$. If $\alpha_\lambda: H \to G_{M_\lambda}$ is the natural homomorphism with kernel M_λ, then $\alpha_\lambda\theta_\lambda$ is a homomorphism from H to G_M. If $\alpha_\lambda\theta_\lambda = \alpha_\mu\theta_\mu$, then $M_\lambda = \mathrm{Ker}(\alpha_\lambda\theta_\lambda) = \mathrm{Ker}(\alpha_\mu\theta_\mu) = M_\mu$. Hence the $\alpha_\lambda\theta_\lambda$ constitute an uncountable set of homomorphisms from the 2-generator group H to the countable group G_M; but this is plainly absurd. □

Notice that the groups we have constructed are 2-generator soluble groups of derived length 3 belonging to the variety of groups G satisfying $[G'', G] = 1$.

Finitely Presented Groups

Recall from 2.2 that a group G is finitely presented if it has a presentation with a finite number of generators and a finite number of relations: equivalently $G \simeq F/R$ where F is a free group of finite rank and R is the normal closure of a finite subset. Certainly there are up to isomorphism only countably many possibilities for F and R, and therefore for G. Therefore the following is clear.

14.1.2. *There exist only countably many nonisomorphic finitely presented groups.*

Theorems 14.1.1 and 14.1.2 taken together show that there exist finitely generated groups which are not finitely presented, but they do not provide an explicit example. In practice it can be a troublesome business to decide whether a particular finitely generated group is finitely presented. On occasion the following lemma is useful in this connection.

14.1.3 (P. Hall). *Let G be a finitely generated group, let $N \lhd G$ and suppose that G/N is finitely presented. Then N is the normal closure in G of a finite subset; thus N is finitely generated as a G-operator group.*

Proof. Let $\theta: F \to G$ be a presentation of G where F is a free group of finite rank. Write S for the preimage of N under θ. Then $S \rightarrowtail F \twoheadrightarrow G/N$ is a presentation of the finitely generated group G/N. By 2.2.3 the subgroup S is the normal closure in F of some finite subset. Applying θ to S we obtain the required result. □

Let us illustrate the utility of this simple result by proving that a particular group is not finitely presented.

14.1.4. *The standard wreath product of two infinite cyclic groups is a 2-generator metabelian group that is not finitely presented.*

Proof. Let H denote the group constructed during the proof of 14.1.1. It was remarked that H/X' is a wreath product of the type under discussion. If this group were finitely presented, 14.1.3 would show X' to be finitely generated—here it is relevant that X' is central in H. But this is certainly not the case. □

This example should be contrasted with the known theorem that every polycyclic group is finitely presented (2.2.4). We mention without going into details that an important geometrical approach to finite presentability of soluble groups has been devised by Bieri and Strebel (see [a202]).

Finite presentability has relatively little effect on the structure of a group or on the types of subgroup that can occur. A deep theorem of G. Higman tells us what kind of subgroups to expect.

A countable group which has a presentation with a recursively enumerable set of relators can be embedded in a finitely presented group. Here the meaning of the term "recursively enumerable" is, roughly speaking, that there is an algorithmic process which will enumerate the relators. A simplified treatment of this theorem is to found in [b43].

The Deficiency of a Group

Let G be a finitely presented group. Suppose that there is a presentation of G with n generators and r relators. The integer $n - r$ is called the *deficiency* of the presentation; it can sometimes be used to yield information about structure of the group that would otherwise be hard to obtain. If $r > 0$, it is possible to add further relators that are consequences of the original ones, so that a presentation of smaller deficiency is obtained. Thus one seeks presentations with as large deficiency as possible.

With this in mind we define the *deficiency of the group G*

$$\operatorname{def} G$$

to be the maximum deficiency of a finite presentation of G. That this is always finite will follow from the next result, which connects the deficiency with the Schur multiplicator. Recall that $d(G)$ is the minimum number of elements required to generate a finitely generated group G.

14.1.5 (P. Hall). *If G is a finitely presented group, the Schur multiplicator $M(G)$ is finitely generated*: *moreover*

$$\operatorname{def} G \leq r_0(G_{ab}) - d(M(G)).$$

In particular G has finite deficiency.

Proof. *Let* $R \rightarrowtail F \twoheadrightarrow G$ be a finite presentation of G with n generators and r relators. Thus R is the normal closure in F of a set of r elements, which means that $R/[R, F]$ can be generated by r elements and thus $d(R/[R, F]) \leq r$. Now $R/R \cap F'$ is isomorphic with a subgroup of the free abelian group F_{ab}, so it is free abelian (4.2.3). It follows from 4.2.5 that $(R \cap F')/[R, F]$ is a direct factor of $R/[R, F]$. Recall that $(R \cap F')/[R, F]$ is isomorphic with $M(G)$—this is Hopf's formula (11.4.15). Consequently $R/[R, F] \simeq M(G) \oplus S$ where $S \simeq RF'/F'$. Now $d(M(G) \oplus S) = d(M(G)) + d(S)$, by Exercise 4.2.4. Hence

$$r \geq d(R/[R, F]) = d(M(G)) + d(S).$$

But $d(S) = r_0(RF'/F') = r_0(F_{ab}) - r_0(F/RF')$, by Exercise 4.2.7, so that $d(S) = n - r_0(G_{ab})$. Therefore

$$r \geq d(M(G)) + n - r_0(G_{ab}),$$

whence $n - r \leq r_0(G_{ab}) - d(M(G))$. This holds for every finite presentation of G. □

Let us see how the inequality of 14.1.5 can be used to give structural information about groups with special presentations. The following is a good example of the use of homological methods to prove a purely group-theoretic theorem.

14.1.6 (Magnus). *Let G be a group having a finite presentation with $n + r$ generators and r relators. If G_{ab} can be generated by n elements $x_1 G', \dots, x_n G'$, then $x_1, \dots, x_n$ generate a free subgroup of rank n for which they form a set of free generators.*

This has the following consequence:

14.1.7 (Magnus). *Let G be a group having a finite presentation with $n + r$ generators and r relators. If G can be generated by n elements, then G is a free group of rank n.*

To see that this is at least plausible imagine that the relators could be used to eliminate r of the $n + r$ generators; it would seem reasonable that the remaining n generators ought not to be subject to any relations. Of course this is no proof since it is not clear that the elimination can be carried out.

***Proof of* 14.1.6.** Using 14.1.5 we derive the inequalities

$$n = n + r - r \leq \operatorname{def} G \leq r_0(G_{ab}) - d(M(G)) \leq n - d(M(G)),$$

which tells us immediately that $d(M(G)) = 0$ and $r_0(G_{ab}) = n$; hence $M(G) = 0$. Moreover Exercise 4.2.3 shows that G_{ab} is a free abelian group of rank n; for $r_0(G_{ab}) = n \leq d(G_{ab}) \leq n$.

Let F be the free group on a set of n elements $\{y_1, \dots, y_n\}$. Then there is a homomorphism $\theta\colon F \to G$ such that $y_i^\theta = x_i$. We shall prove that θ is injective, which will establish the theorem.

In the first place θ maps F_{ab} onto G_{ab} because the x_iG' generate G_{ab}. Since both F_{ab} and G_{ab} are free abelian groups of rank n, it follows easily that θ maps F_{ab} isomorphically onto G_{ab}.

Let $F_i = F/\gamma_{i+1}F$ and $G_i = G/\gamma_{i+1}G$. Assume that θ maps F_i isomorphically onto G_i—note that when $i = 1$ this has just been proved. Consider the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \gamma_{i+1}F & \longrightarrow & F & \longrightarrow & F_i & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} & & \\ 1 & \longrightarrow & \gamma_{i+1}G & \longrightarrow & G & \longrightarrow & G_i & \longrightarrow & 1. \end{array}$$

Here the down maps on the left and right are induced by θ. Applying 11.4.17 we obtain a corresponding commutative homology diagram with exact rows

$$\begin{array}{ccccccccccc} 0 = M(F) & \longrightarrow & M(F_i) & \xrightarrow{\alpha} & \gamma_{i+1}F/\gamma_{i+2}F & \xrightarrow{\beta} & F_{ab} & \xrightarrow{\gamma} & (F_i)_{ab} & \longrightarrow & 1 \\ \downarrow{\scriptstyle\theta_*} & & \downarrow{\scriptstyle\theta_*} & & \downarrow{\scriptstyle\theta_*} & & \downarrow{\scriptstyle\theta_*} & & \downarrow{\scriptstyle\theta_*} & & \\ 0 = M(G) & \longrightarrow & M(G_i) & \xrightarrow{\alpha'} & \gamma_{i+1}G/\gamma_{i+2}G & \xrightarrow{\beta'} & G_{ab} & \xrightarrow{\gamma'} & (G_i)_{ab} & \longrightarrow & 1. \end{array}$$

Here $M(F) = 0$ because F is a free group (11.3.2). Since $\theta\colon F_i \to G_i$ is bijective, so is the induced map $\theta_*\colon M(F_i) \to M(G_i)$; here we use the fact that $1 = (\theta\theta^{-1})_* = \theta_*(\theta^{-1})_*$ by Exercise 11.4.16. In addition $\theta_*\colon (F_i)_{ab} \to (G_i)_{ab}$ is bijective. Our immediate object is to prove that $\theta_*\colon \gamma_{i+1}F/\gamma_{i+2}F \to \gamma_{i+1}G/\gamma_{i+2}G$ is bijective: for this will surely imply that $\theta_*\colon F_{i+2} \to G_{i+2}$ is bijective. (The reader with a grounding in homological algebra will recognize this as the "five lemma" and may skip the next two paragraphs.) In fact $\beta = 0 = \beta'$.

Let x belong to the kernel of the above θ_*. Then $1 = x^{\theta_*\beta'} = x^{\beta\theta_*}$ by commutativity of the diagram. Hence $x^\beta = 1$ and $x \in \operatorname{Ker}\beta = \operatorname{Im}\alpha$; thus $x = y^\alpha$ where $y \in M(F_i)$. Hence $1 = x^{\theta_*} = y^{\alpha\theta_*} = y^{\theta_*\alpha'}$, so that $y^{\theta_*} = 1$ and $y = 1$. Thus $x = 1$ and the θ^* in question is injective.

Now for surjectivity. Let $a \in \gamma_{i+1}G/\gamma_{i+2}G$; then $a^{\beta'} = b^{\theta_*}$ for some $b \in F_{ab}$ since $\theta_*\colon F_{ab} \to G_{ab}$ is surjective. Hence $1 = a^{\beta'\gamma'} = b^{\theta_*\gamma'} = b^{\gamma\theta_*}$, which yields $b^\gamma = 1$ since $\theta_*\colon (F_i)_{ab} \to (G_i)_{ab}$ is injective. Therefore $b \in \operatorname{Ker}\gamma = \operatorname{Im}\beta$ and $b = c^\beta$ for some c in $\gamma_{i+1}F/\gamma_{i+2}F$. Thus $a^{\beta'} = b^{\theta_*} = c^{\beta\theta_*} = c^{\theta_*\beta'}$ and $a \equiv c^{\theta_*}$ mod($\operatorname{Ker}\beta' = \operatorname{Im}\alpha'$). It follows that $a = c^{\theta_*}d^{\alpha'}$ for some $d \in M(G_i)$. But $d = e^{\theta_*}$ for some e in $M(F_i)$. Hence $d^{\alpha'} = e^{\theta_*\alpha'} = e^{\alpha\theta_*}$ and $a = (ce^\alpha)^{\theta_*}$, which proves surjectivity.

It now follows by induction on i that $\theta_*\colon F/\gamma_{i+1}F \to G/\gamma_{i+1}G$ is bijective for all i. Hence $\operatorname{Ker}\theta \le \gamma_{i+1}F$ for all i. But the intersection of all the $\gamma_{i+1}F$'s is 1, by 6.1.10. Hence $\operatorname{Ker}\theta = 1$ and $\theta\colon F \to G$ is injective. □

EXERCISES 14.1

1. A group G is said to have finite *torsion-free rank* if it has a series of finite length whose factors are either torsion or infinite cyclic. Prove that all series in G of this type have the same number of infinite cyclic factors. (This number is called the *torsion-free rank* or *Hirsch length* of G, see 4.2.)
2. Prove that a group has finite torsion-free rank r if and only if it has a *normal* series whose factors are torsion groups or torsion-free abelian groups the sum of whose ranks equals r. [*Hint*: To prove necessity form a series as in Exercise 14.1.1 and take the normal closure of the smallest nontrivial term.]
3. A group G has *finite Prüfer rank* r if every finitely generated subgroup can be generated by r elements and r is the least such integer. Prove that the class of groups of finite Prüfer rank is closed with respect to forming subgroups, images and extensions.
4. Show that a soluble group has finite Prüfer rank if and only if it has a series of finite length whose factors are either infinite cyclic or isomorphic with subgroups of $\mathbb{Q}/\mathbb{Z}$. Deduce that a soluble group of finite Prüfer rank has finite torsion-free rank.
5. Let G be a finitely presented group. Prove that every quotient of G is finitely presented if and only if G satisfies max-n.
6. If r is an integer > 1, show that the standard wreath product $\mathbb{Z} \wr \mathbb{Z} \wr \cdots \wr \mathbb{Z}$ with r factors is finitely generated but not finitely presented.
7. If G is a finitely presented group with positive deficiency d, show that G has a free abelian quotient group of rank d.
8. A finite presentation is said to be *balanced* if it has the same number of generators as relators. If a torsion group G has a balanced presentation, prove that $M(G) = 0$.
9. Prove that a finite abelian group has a balanced presentation if and only if it is cyclic.
10. Let $G = \langle x_1, x_2, \dots, x_n | u \rangle$ be a "one-relator group". Let e_i be the sum of the exponents of x_i in u (regarded as a word in the x_i). If $e_1, e_2, \dots, e_n$ are coprime, show that G has a free subgroup of rank $n - 1$. [*Hint*: Prove that G_{ab} is free abelian of rank $n - 1$.]

14.2. Torsion Groups and the Burnside Problems

According to the definition in 12.1, a group is *locally finite* if each finitely generated subgroup is finite. Thus a locally finite group is a torsion group. To pose the converse is to ask if every finitely generated torsion group is finite. This is a famous problem named after Burnside, who first raised it in an article in 1902 ([a20]).

The Burnside problem remained unsolved until 1964 when Golod constructed a finitely generated infinite p-group using class field theory. Since then many other such groups have been found. For example, in 1980 Grigorčuk [a61] gave an example of an infinite 3-generator 2-group which is a group of transformations of the interval [0, 1]. Also Gupta and Sidki [a66] constructed an infinite 2-generator p-group consisting of automorphisms of the infinite regular tree of degree p.

Here we shall construct an infinite 2-generator p-group, using only elementary properties of free products. The construction is due to Gupta.

Construction

Let p be an odd prime (when $p = 2$, the construction requires modification —see Exercise 14.2.7). Consider first the free product

$$H = \langle a \rangle * \langle t \rangle$$

where a and t have order p. If we put $a_i = a^{t^i}$, then

$$A = a^H = \langle a_0, a_1, \dots, a_{p-1} \rangle.$$

It is easily seen that the expression $a_{i_1}^{l_1} a_{i_2}^{l_2} \cdots a_{i_r}^{l_r}$, where $i_j \neq i_{j+1}$, is a normal form for elements of A. Thus by 6.2.4 the group A is a free product:

$$A = \langle a_0 \rangle * \langle a_1 \rangle * \cdots * \langle a_{p-1} \rangle.$$

Also of course $H = \langle t \rangle \ltimes A$.

Next for $k = 0, 1, \dots, p - 1$ a homomorphism θ_k: $A \to H$ is defined by the rules

$$a_k^{\theta_k} = a_0 \quad \text{and} \quad a_i^{\theta_k} = t^{i-k} \quad \text{if} \quad i \neq k.$$

These θ_k are used to define subgroups as follows: $N_0 = 1$ and

$$N_{i+1} = \{ w \in A \mid w^{\theta_k} \in N_i, \forall k \}.$$

Thus, for example, $N_1 = \bigcap_{k=0,1,2,\dots} \operatorname{Ker} \theta_k$. An easy induction on i shows that $N_i \leq N_{i+1}$, so that $1 = N_0 \leq N_1 \leq N_2 \leq \cdots$.

Induction can also be used to prove that $N_i \lhd H$. Indeed suppose that $N_{i-1} \lhd H$. Now it follows at once from the definition that $N_i \lhd A$. Also, if $w = w(a_0, a_1, \dots, a_{p-1}) \in N_i$, then, since $a_j^{\theta_k} = a_{j-1}^{\theta_{k-1}}$, we have for all k that

$$\begin{aligned}(t^{-1}wt)^{\theta_k} &= (w(a_1, a_2, \dots, a_{p-1}, a_0))^{\theta_k} \\ &= (w(a_0, a_1, \dots, a_{p-1}))^{\theta_{k-1}} \in N_i^{\theta_{k-1}} \leq N_{i-1}.\end{aligned}$$

Hence $t^{-1}wt \in N_i$ and $N_i \lhd N$.

To complete the construction put $N = \bigcup_{i=1,2,\dots} N_i$ and write

$$G = H/N.$$

Concerning this group we shall prove

14.2.1. *The group G is an infinite p-group with two generators.*

Proof. Obviously G is a 2-generator group. The main step in the proof consists in showing that G is a p-group. First comes a definition. Let $h \in H$ and write $h = t^i w$ where $w \in A$. The *length* $l(h)$ of h is defined by

$$l(h) = \begin{cases} 1 + l(w) & \text{if } i \not\equiv 0 \pmod{p}, \\ l(w) & \text{if } i \equiv 0 \pmod{p}, \end{cases}$$

where $l(w)$ is the length of the normal form of w. We shall prove that

$$h^{p^n} \in N_n$$

provided that $n \geq l(h)$; this will show that G is a p-group.

The proof is by induction on $l(h)$. If $l(h) \leq 1$, then $h \in \langle t \rangle$ or $h \in \langle a_i \rangle$ for some i, in which case $h^p = 1$. Assume that the statement is true for elements of length n, and let $h = t^i w$ have length $n + 1$.

First of all consider the case where $i \not\equiv 0 \pmod{p}$. Then $l(w) = n$. Now

$$h^p = (t^i w)^p = w^{t^{i(p-1)}} w^{t^{i(p-2)}} \cdots w^{t^i} w$$

since $t^p = 1$. In addition, if $w = w(a_0, a_1, \ldots, a_{p-1})$, then $w^{t^{i(p-j)}} = w(a_{i(p-j)}, a_{1+i(p-j)}, \ldots, a_{p-1+i(p-j)})$ where subscripts are to be reduced modulo p. Suppose that a_k occurs as a power exactly d_k times in w. Then a_k occurs as a power in h^p at most $\sum_{r=0}^{p-1} d_{k-ir} = \sum_{r=0}^{p-1} d_r \leq n$ times (again subscripts are reduced modulo p).

Now consider $(h^p)^{\theta_k}$. This involves at most n a_0's, and also various power of t. If the exponent sum of a_r in w is l_r, then for $r \neq k$ the contribution of a_r to the exponent of t in $(h^p)^{\theta_k}$ is

$$\sum_{j=0}^{p-1} l_r(r + ij - k) = l_r\left(p(r - k) + i\binom{p}{2}\right) \equiv 0 \pmod{p}$$

since $p > 2$. Moving all powers of t to the left in $(h^p)^{\theta_k}$, we see that $(h^p)^{\theta_k} \in A$ and this involves at most n powers of a_i's, i.e., $l((h^p)^{\theta_k}) \leq n$. By induction on n we have $((h^p)^{\theta_k})^{p^n} \in N_n$, so that $(h^{p^{n+1}})^{\theta_k} \in N_n$ for all k, and $h^{p^{n+1}} \in N_{n+1}$.

Now consider the case where $i \equiv 0 \pmod{p}$ and $h = w \in A$; here $l(w) = n + 1$. Since we can replace w by a conjugate, there is no loss in supposing that w does not begin and end with the same generator a_j. If $l(w^{\theta_k}) \leq n$ for all k, then induction will show that $(w^{\theta_k})^{p^n} \in N_n$ so that $w^{p^n} \in N_{n+1}$, and $w^{p^{n+1}} \in N_{n+1}$. Thus we can assume that $l(w^{\theta_k}) = n + 1$ for some k.

It follows that w cannot involve two or more powers a_j^r with $j \neq k$. Hence, taking into account the fact that w does not begin and end with the same a_j, we see that $l(w) = 2$ and $n = 1$. Also, conjugating if necessary, we can suppose that $w = a_j^r a_k^s$ where $j \neq k$. Then $w^{\theta_k} = t^{(j-k)r} a_0^s$.

Arguing as in the case $a \not\equiv 0 \pmod{p}$, we can conclude that $((w^{\theta_k})^p)^{\theta_l}$ in A has length 1 at most. Consequently $(w^{p^2})^{\theta_k \theta_l} = 1$ for all l, and $(w^{p^2})^{\theta_k} \in N_1$. Also $(w^{p^2})^{\theta_l} \in N_1$ for $l \neq k$, so $w^{p^2} \in N_2$, as required.

It remains to prove that $G = H/N$ is an infinite group. Assume that this is false; then N is finitely generated and $N = N_i$ for some i.

To disprove this, we introduce elements $v_0, v_1, v_2, \ldots$ of A via the following equations:

$$v_0 = [a_0, a_1], \qquad v_{i+1} = [a_0, v_i].$$

Then $v_0^{\theta_0} = [a_0, t] = a_0^{-1}a_1$, and an easy induction on i shows that $v_{i+1}^{\theta_0} = v_i$. By 6.2.5 the element v_j has infinite order; for its normal form begins with a_0^{-1} and ends with a_1.

We shall argue that $\langle v_j \rangle \cap N_{j+2} = 1$ for all j. This will contradict $N = N_i$ since $v_i^{p^l} \in N_l$ where $l = l(v_i)$. Suppose that $\langle v_{j-1} \rangle \cap N_{j+1} = 1$ and that some v_j^r belongs to N_{j+2}. Then $(v_j^{\theta_0})^r = (v_j^r)^{\theta_0} \in N_{j+1}$, and so $v_{j-1}^r \in \langle v_{j-1} \rangle \cap N_{j+1} = 1$. Since v_{j-1} has infinite order, $r = 0$ and $v_j^r = 1$. Hence it is enough to prove that $\langle v_0 \rangle \cap N_2 = 1$. Assume that $v_0^r \in N_2$. Then $(v_0^r)^{\theta_0} = (a_0^{-1}a_1)^r \in N_1$. Hence $1 = ((a_0^{-1}a_1)^r)^{\theta_0} = (a_0^{-1}t)^r$, which shows that $r \equiv 0 \pmod p$. Therefore

$$1 = ((a_0^{-1}t)^p)^{r/p} = (a_1 a_2 \cdots a_{p-1} a_0)^{-r/p}.$$

But this implies that $r = 0$, so the proof is complete. □

In his original memoir of 1902 Burnside also raised a special case of the preceding problem: does a finitely generated group of finite exponent have to be finite? If G is an n-generator group and $G^e = 1$, then G is an image of the so-called *free Burnside group*

$$B(n, e) = F/F^e$$

where F is a free group with n generators; this follows from 2.3.7. In the terminology of 2.2 the group $B(n, e)$ is a free group in the variety of groups of exponent dividing e. Thus Burnside's question is whether $B(n, e)$ is finite.

Our present state of knowledge of this problem is very incomplete. If $e = 1$ or $n = 1$, it is trivially true. If $e = 2, 3, 4$ or 6, it has been proved with varying degrees of difficulty. At present no other values of e are known for which $B(n, e)$ is finite.

On the other hand, in 1968 Novikov and Adjan, in a series of papers of great length, proved that $B(n, e)$ is infinite if $n > 1$ and e is a large enough odd number. Subsequently work of Adjan showed that $B(n, e)$ is infinite if $n > 1$ and e is an odd integer ≥ 665 (see [b1]). Very recently Ivanov has proved that $B(n, e)$ is infinite for $n > 1$ and all sufficiently large exponents e, whether even or odd.

We shall examine the cases $e = 2, 3, 4$ here: to prove that $B(n, 6)$ is finite is much harder (see M. Hall [b31]).

14.2.2. *$B(n, 2)$ is finite with order 2^n.*

Proof. If G is an n-generator group and $G^2 = 1$, then for any x, y we have $1 = (xy)^2 = xyxy$, so that $xy = y^{-1}x^{-1} = yx$. Hence G is an elementary abelian 2-group of rank $\leq n$ and $|G| \leq 2^n$. But an elementary abelian 2-group with rank n has order 2^n, so $|B(n, 2)| = 2^n$. □

14.2.3 (Levi–van der Waerden). $B(n, 3)$ *is finite and has order* 3^d *where* $d \leq n + \binom{n}{2} + \binom{n}{3}$.

Proof. Let G be a group such that $G^3 = 1$ and let $x_1, \ldots, x_n$ generate G. Since G_{ab} is obviously an elementary abelian 3-group, $|G_{ab}| \leq 3^n$. Moreover by 5.1.7 the group $G'/[G', G]$ is generated by all the $[x_i, x_j][G', G]$ where $i < j$; hence $|G' : [G', G]| \leq 3^{\binom{n}{2}}$. By 12.3.5 and 12.3.6 the group G is nilpotent of class at most 3. Hence $[G', G]$ is contained in the center of G, so it may be generated by the $\binom{n}{3}$ commutators $[x_i, x_j, x_k]$ where $i < j < k$: here it is relevant that $[x, y, z] = [z, x, y]$ holds identically in G (by 12.3.6). Thus $|[G', G]| \leq 3^{\binom{n}{3}}$ and the result follows. □

In fact the order of $B(n, 3)$ equals $3^{n+\binom{n}{2}+\binom{n}{3}}$ – a proof is sketched in Exercise 14.2.4.

14.2.4 (Sanov). $B(n, 4)$ *is finite.*

The proof is based on a lemma which is a special case.

14.2.5. *Let G be a group such that $G^4 = 1$. Suppose that H is a finite subgroup and x is an element of G such that $G = \langle x, H \rangle$ and $x^2 \in H$. Then G is finite.*

Proof. Since $x^2 \in H$, an arbitrary element g of G can be written in the form

$$g = h_1 x h_2 x \cdots h_{n-1} x h_n \tag{2}$$

where $h_i \in H$. Suppose that (2) is an expression for g of shortest length. If we can bound n in terms of $|H|$, it will follow that G is finite.

If h is any element of H, then $(xh)^4 = 1$, so that

$$xhx = h^{-1}x^{-1}h^{-1}x^{-1}h^{-1} = h^{-1}x(x^2h^{-1}x^2)xh^{-1}$$

since $x^4 = 1$. Thus

$$xhx = h^{-1}xh^*xh^{-1} \tag{3}$$

where $h^* \in H$. Applying this rule to xh_ix in (2) we obtain

$$g = h_1 x h_2 x \cdots x h_{i-2} x (h_{i-1} h_i^{-1}) x h_i^* x (h_i^{-1} h_{i+1}) x \cdots x h_{n-1} x h_n \tag{4}$$

with h_i^* in H. Note that this expression still has the minimal length n. Thus we have succeeded in replacing h_{i-1} by $h_{i-1}h_i^{-1}$. Similarly we may apply the rule (3) to the element $x(h_{i-1}h_i^{-1})x$ in (4) to obtain an expression for g of length n in which h_{i-2} is replaced by $h_{i-2}h_ih_{i-1}^{-1}$. By repeated application of

this process we may replace h_2 by any of the expressions

$$h_2h_3^{-1},\ h_2h_4h_3^{-1},\ h_2h_4(h_3h_5)^{-1},\ h_2h_4h_6(h_3h_5)^{-1},\ldots.$$

Notice that there are $n-2$ of these elements. Suppose that $n-2>|H|$. Then at least two of the above elements are equal. For example, suppose that

$$h_2h_4\cdots h_{2r}(h_3h_5\cdots h_{2r+1})^{-1}=h_2h_4\cdots h_{2s}(h_3h_5\cdots h_{2s+1})^{-1}$$

where $r<s$. Then

$$h_{2r+2}\cdots h_{2s}(h_{2r+3}\cdots h_{2s+1})^{-1}=1. \tag{5}$$

The left-hand side of (5) is one of the expressions which we may substitute for h_{2r+2}; it can therefore be deleted from the expression for g, which contradicts the minimality of n. In the same way equality of expressions of other types leads to a contradiction. Consequently $n\leq|H|+2$. □

***Proof of* 14.2.3.** This is now an easy matter. Let $G=\langle x_1,\ldots,x_n\rangle$ satisfy $G^4=1$. If $n=1$, then it is clear that $|G|\leq 4$. Let $n>1$ and assume that $H=\langle x_1,\ldots,x_{n-1}\rangle$ is finite. By 14.2.5 the subgroup $K=\langle H,x_n^2\rangle$ is finite. The same result shows that $G=\langle K,x_n\rangle$ is finite. The theorem now follows by induction on n. □

The exact order of $B(n,4)$ is unknown, although the proof of 14.2.4 gives a crude upper bound (see Exercise 14.2.1). However, it is known that the groups $B(2,4)$, $B(3,4)$, and $B(4,4)$ have orders 2^{12}, 2^{69}, and 2^{422} respectively. Also it has been shown by Razmyslov that there are insoluble groups of exponent 4 ([a162]).

The Restricted Burnside Problem

This is the problem: does there exist an upper bound $f(n,e)$ for the order of a finite n-generator group of exponent dividing e? A positive answer would mean that finite quotients of $B(n,e)$ have bounded order, so that there is in effect a largest finite quotient; however, $B(n,e)$ itself might conceivably be infinite.

We shall establish the truth of the conjecture for e dividing 6.

14.2.6. *The order of a finite n-generator group G of exponent dividing* 6 *cannot exceed a certain integer depending only on n.*

Proof. In the first place G is soluble by the Burnside p-q Theorem (8.5.3). Also $l_2(G)\leq c_2(G)$ by 9.3.7. Since a Sylow 2-subgroup of G has exponent 2, it is abelian and $c_2(G)\leq 1$. Hence $l_2(G)\leq 1$, which means that $G=O_{2'22'}(G)$.

Now $G/O_{2'2}(G)$ is a 2'-group of exponent dividing 6, so it has exponent dividing 3. By 14.2.3 the order of $G/O_{2'2}(G)$ cannot exceed $3^{n+\binom{n}{2}+\binom{n}{3}}$. It follows from the Reidemeister–Schreier Theorem (6.1.8) that $O_{2'2}(G)$ can be generated by $l = (n-1)3^{n+\binom{n}{2}+\binom{n}{3}} + 1$ elements. Next $O_{2'2}(G)/O_{2'}(G)$ is an elementary abelian 2-group; thus its order cannot exceed 2^l. Consequently $O_{2'}(G)$ can be generated by $m = (l-1)2^l + 1$ elements. Finally $O_{2'}(G)$ has exponent dividing 3, so its order does not exceed $3^{n+\binom{m}{2}+\binom{m}{3}}$. Thus we have an upper bound for $|G|$. □

Actually the maximum order of a finite n-generator group with exponent dividing 6 is

$$2^a 3^{b+\binom{b}{2}+\binom{b}{3}} \tag{6}$$

where

$$a = (n-1)3^{n+\binom{n}{2}+\binom{n}{3}} \quad \text{and} \quad b = (n-1)2^n + 1.$$

Since M. Hall has confirmed that $B(n, 6)$ is finite, the integer (6) is in fact the order of this free Burnside group.

Quite recently Zel'manov, in a remarkable paper, has shown that the restricted Burnside problem has a positive solution for all exponents. For an accessible account of the proof see [b70].

EXERCISES 14.2

1. Find a function $f(n)$ (defined recursively) such that $|B(n, 4)| \leq f(n)$.

2. If F is a free group, prove that F/F^4 is nilpotent if and only if F has finite rank.

3. Find a 2-generator group of exponent 4 and order 128 and a 2-generator group of exponent 8 and order 2^{136}. [*Hint*: If F is a free group with rank 2, consider $F/(F^2)^2$ and $F/((F^2)^2)^2$.]

4. (Levi and van der Waerden: see also [b26]). Show that the order of $B(n, 3)$ is $3^{n+\binom{n}{2}+\binom{n}{3}}$ by means of the following procedure.
   (a) It suffices to prove that $|B(3, 3)| = 3^7$ (see the proof of 14.2.3).
   (b) Let $A = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \times \langle d \rangle$ be an elementary abelian group of order 3^4. Let $t \in \operatorname{Aut} A$ be given by $a^t = ad$ and $[b, t] = [c, t] = [d, t] = 1$. Then $H = \langle t \rangle \ltimes A$ has exponent 3 and order 3^5.
   (c) Define $u \in \operatorname{Aut} H$ by $t^u = tc$, $b^u = bd^{-1}$ and $1 = [a, u] = [c, u] = [d, u]$. Then $K = \langle u \rangle \ltimes H$ has exponent 3 and order 3^6.
   (d) Define $v \in \operatorname{Aut} K$ by $u^v = ua^{-1}$, $t^v = tb^{-1}$, $c^v = cd$ and $1 = [a, v] = [b, v] = [d, v]$. Then $G = \langle v \rangle \ltimes K$ has exponent 3 and order 3^7.
   (e) Show that $G = \langle t, u, v \rangle$.

5. Find a 2-generator group of exponent 9 and order 3^{3685}

6. Prove that the group G of 14.2.1 is not finitely presented.

7. Show that the construction leading to 14.2.1 can be modified to allow p to equal 2. [*Hint*: Let a and t have order 4. Define $a_k^{\theta_k} = a_0$, $a_i^{\theta_k} = t^{i-k}$ if $i \not\equiv k \pmod 2$, and $a_i^{\theta_k} = 1$ if $i \equiv k \pmod 2$, $i \neq k$.]

14.3. Locally Finite Groups

Of the finiteness properties that have been encountered the one which seems closest to finiteness is surely the property of being locally finite. To test this intuitive judgment one may inquite whether any of the major theorems of finite group theory can be carried over, with suitable modifications, to locally finite groups. One of the objectives of this section will be to examine how far Sylow's Theorem is valid for locally finite groups.

To begin with, a simple observation: obviously the class of locally finite groups is closed with respect to forming subgroups and images. It is not hard to see that it is also extension closed.

14.3.1 (Schmidt). *If $N \lhd G$ and the groups N and G/N are both locally finite, then G is locally finite.*

Proof. Let H be a finitely generated subgroup of G. Then $H/H \cap N \simeq HN/N$, which is finite. By the Reidmeister–Schreier Theorem—or more simply by 1.6.11—the subgroup $H \cap N$ is finitely generated, and thus finite. Therefore H is finite. □

Sylow Subgroups in Locally Finite Groups

If p is a prime, a *Sylow p-subgroup* of a possibly infinite group G is defined to be a maximal p-subgroup. It is an easy consequence of Zorn's Lemma that *every p-subgroup of G is contained in a Sylow p-subgroup.* In particular, Sylow p-subgroups always exist. It follows from Sylow's Theorem that if G is finite, then a maximal p-subgroup of G has order equal to the largest power of p dividing $|G|$. This demonstrates that the foregoing definition is consistent with the notion of a "Sylow p-subgroup of a finite group" introduced in 1.6.

The main problem of Sylow theory is to determine whether all the Sylow p-subgroups of a group are conjugate, possibly in some weak sense. Of course, this is true for finite groups by Sylow's Theorem. However, conjugacy tends to fail in a spectacular manner for infinite groups. Indeed Sylow p-subgroups need not even be isomorphic!

Let us begin with the remark that the proof of Sylow's Theorem given in Chapter 1 does not require the finiteness of the whole group. In fact the argument establishes the following result.

14.3.2 (Dicman–Kuroš–Uzkov). *Let P be a Sylow p-subgroup of a group G and suppose that P has only finitely many conjugates in G. Then every Sylow p-subgroup of G is conjugate to P. Moreover their number is congruent to 1 modulo p.*

It is intructive to see how badly Sylow's Theorem can fail for infinite groups.

14.3.3. *Let P_1 and P_2 be arbitrary p-groups and let $G = P_1 * P_2$ be their free product. Then P_1 and P_2 are Sylow p-subgroups of G. Hence in an infinite group Sylow p-subgroups can have different cardinalities and thus need not be conjugate.*

Proof. Let P be a Sylow p-subgroup of G containing P_1. Then P cannot be a free product of nontrivial groups; otherwise it would contain an element of infinite order, by 6.2.5. Hence the Kuroš Subgroup Theorem (6.3.1) shows that P is conjugate to a subgroup of P_1 or P_2. However one can tell from the normal form for elements of a free product that a nontrivial element of P_1 cannot be conjugate to an element of P_2. Consequently P is conjugate to a subgroup of P_1, say $P = P_0^g$ where $P_0 \leq P_1$. Now $P \leq P_1^g \leq P^g$, which implies that $P = P^g$ because P is a Sylow p-subgroup. Therefore $P^g = P = P_0^g$ and $P = P_0 \leq P_1$. Hence $P = P_1$. □

From now on we shall consider only locally finite groups, hoping for better behavior on the part of the Sylow subgroups.

14.3.4. *Let G be a locally finite group and suppose that P is a finite Sylow p-subgroup of G. Then all Sylow p-subgroups of G are finite and conjugate.*

Proof. Let P_1 be any finite p-subgroup of G. Then $H = \langle P, P_1 \rangle$ is finite because G is locally finite. Now clearly P is a Sylow p-subgroup of H, so Sylow's Theorem shows that P_1 is contained in some conjugate of P. In particular $|P_1| \leq |P|$ and no finite p-subgroup can have order larger than $|P|$. It follows that a Sylow p-subgroup is necessarily finite. The argument already given shows that any Sylow p-subgroup is conjugate to P. □

The next theorem is much deeper; it does a good deal to elucidate the question of conjugacy of Sylow p-subgroups in countable locally finite groups.

14.3.5 (Asar). *Let G be a locally finite group. If each countable subgroup of G has only countably many Sylow p-subgroups, then all the Sylow p-subgroups of G are conjugate.*

Proof. We presume the theorem to be false, reaching a contradiction in three steps.

(i) *There is a Sylow p-subgroup P with the property: each finite subgroup of P is contained in at least two Sylow p-subgroups of G.* By assumption there exist two Sylow p-subgroups P and Q which are not conjugate. Suppose that P does not have the property in question: the idea is to prove that

Q *does* have this property. To this end let Y be a finite subgroup of Q. By hypothesis, P has a finite subgroup X which is contained in only one Sylow p-subgroup, namely P itself. Then $L = \langle X, Y \rangle$ is finite. Now $P \cap L$ is contained in a Sylow p-subgroup P_1 of L and P_1 contained in a Sylow p-subgroup P_2 of G. Hence $X \leq P \cap L \leq P_1 \leq P_2$; by hypothesis $P_2 = P$ and thus $P_1 = P \cap L$. Therefore $P \cap L$ is a Sylow p-subgroup of L. Consequently $Y \leq (P \cap L)^g \leq P^g$ for some g; but $P^g \neq Q$ because P and Q are not conjugate. Hence Q has the property in question.

(ii) *If X is a finite subgroup of P, there exist a finite subgroup X_0 of P and a conjugate X_1 of X_0 such that $X < X_0$, $X < X_1$ and $\langle X_0, X_1 \rangle$ is not a p-group.* By (i) there is a Sylow p-subgroup $Q \neq P$ such that $X \leq Q$. Let $x \in Q \backslash P$ and put $M = \langle x, X \rangle$. Then $M \leq Q$, so M is a finite p-group. Write $T = P \cap M$. Then $T < M$ and $T < N_M(T)$. It follows that $N_M(T) \nleq N_G(P)$ since otherwise $N_M(T) \leq P$, the latter being the only Sylow p-subgroup of $N_G(P)$. Choose y from $N_M(T) \backslash N_G(P)$. Then $\langle P, P^y \rangle$ cannot be a p-group: for otherwise $P = P^y$ and $y \in N_G(P)$. Hence there is a finite subgroup X_0 of P containing T such that $\langle X_0, X_0^y \rangle$ is not a p-group. Let $X_1 = X_0^y$. Clearly $X \leq T = T^y \leq X_0^y = X_1$. Also $X < X_0$ because $\langle X, X^y \rangle$ is contained in the p-group T.

(iii) *Final step.* Using (ii) repeatedly we can construct for any given finite subgroup X of P and each infinite sequence $\boldsymbol{i} = (i_1, i_2, \ldots)$ of 0's and 1's a chain of finite p-subgroups

$$X < X_{i_1} < X_{i_1 i_2} < \cdots \tag{7}$$

with the property that $\langle X_{i_1 i_2 \ldots i_r j}, X_{i_1 i_2 \ldots i_r k} \rangle$ is never a p-group if $j \neq k$.

Let $X_{\boldsymbol{i}}$ denote the union of the chain (7). If $\boldsymbol{i} \neq \boldsymbol{i}'$, then $X_{\boldsymbol{i}}$ and $X_{\boldsymbol{i}'}$ cannot be contained in the same p-subgroup by the non-p-group property. Now let H be the subgroup generated by all the $X_{\boldsymbol{i}}$ for varying $\boldsymbol{i}$; then H is generated by all the $X_{i_1 i_2 \ldots i_r}$, so it is surely countable. But each sequence $\boldsymbol{i}$ determines a Sylow p-subgroup of H, namely one containing $X_{\boldsymbol{i}}$. Since there are $2^{\aleph_0}$ sequences, there will be that many Sylow p-subgroups of H. However this is contrary to hypothesis. □

Asar's theorem takes a particularly satisfying form for countable locally finite groups.

14.3.6. *Let G be a countable locally finite group. Then the Sylow p-subgroups of G are conjugate if and only if they are countable in number.*

Proof. If all the Sylow p-subgroups are conjugate, the set of Sylow p-subgroups must be countable since G is countable.

Conversely, suppose that G has countably many Sylow p-subgroups. Conjugacy will follow via 14.3.5 if it can be shown that a subgroup H of G has countably many Sylow p-subgroups. Let P be a Sylow p-subgroup of H. Then P is contained in a Sylow p-subgroup Q of G. Now $P \leq Q \cap H \leq H$,

so that $P = Q \cap H$ and P is determined by Q. But there are only countably many Q's. □

The reader is perhaps wondering if Sylow p-subgroups are always conjugate in locally finite groups. However this is not true, even for countable groups.

EXAMPLE. Let G be the (restricted) direct product of a countably infinity of copies of S_3; this is surely a countable locally finite group. If a_i is an element of order 2 in the ith direct factor, then $P = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots$ is a Sylow 2-subgroup of G because any strictly larger subgroup contains an element of order 3. Now each a_i can be chosen in three ways, so there are $2^{\aleph_0}$ choices for P. These cannot all be conjugate since G is countable. □

As a matter of fact there are more sophisticated examples which show that worse situations can arise: the Sylow p-subgroups of a countable locally finite group need not even be isomorphic (Exercise 14.3.6).

There has been much recent work on Sylow theory of locally finite groups: the interested reader may consult [b18].

Infinite Abelian Subgroups of Locally Finite Groups

Does every infinite group have an infinite abelian subgroup? This is a question of some antiquity in the theory of groups, although its origin seems to be obscure. The answer is certainly positive if an element of infinite order is present; thus we can restrict ourselves to torsion groups. It is now known that all the abelian subgroups of the free Burnside group $B(n, e)$ are cyclic if $n > 1$ and $e \geq 665$ is odd; on the other hand $B(n, e)$ is infinite. This is a by-product of the work of Novikov and Adjan on the Burnside problem. Thus the question has in general a negative answer.

We shall show that the situation is quite different for locally finite groups, proving the following celebrated theorem.

14.3.7 (P. Hall–Kulatilaka, Kargapolov†). *Every infinite locally finite group has an infinite abelian subgroup.*

If a group has an infinite abelian subgroup, each element of this subgroup will have infinite centralizer. This suggests that in any attack on 14.3.7 one is going to have to deal with groups in which nontrivial elements have finite centralizers. In fact this is the key to the proof.

The following theorem applies to torsion groups that are not necessarily locally finite.

† Mikhail Ivanovič Kargapolov (1928–1976).

14.3.8 (Šunkov). *Let G be an infinite torsion group. Assume that G contains an involution i such that $C_G(i)$ is finite. Then either the center of G contains an involution or G has a proper infinite subgroup with nontrivial center. In both cases there is a nontrivial element with infinite centralizer.*

This theorem will effectively reduce 14.3.7 to the case where all elements have odd order.

***Proof of* 14.3.8.** We shall suppose the theorem false.

(i) *There are infinitely many elements g in G such that $g^i = g^{-1}$* (let these be called *i-elements*). In the first place there are infinitely many conjugates of i since $|G : C_G(i)|$ must be infinite. Thus G contains infinitely many involutions. Since $C_G(i)$ is finite, there must exist infinitely many distinct cosets $C_G(i)a$ with a an involution. Now $(aa^i)^i = a^ia = (aa^i)^{-1}$, so aa^i is an i-element. If $aa^i = bb^i$, the elements a and b being involutions, then $ab \in C_G(i)$ and $C_G(i)a = C_G(i)b$. Therefore involutions belonging to distinct right cosets of $C_G(i)$ give rise to infinitely many i-elements.

(ii) *G contains only finitely many i-elements of even order.* For suppose that $\{x_1, x_2, \dots\}$ is an infinite set of nontrivial elements of this type. Now there is a positive integer m_r such that $x_r^{m_r}$ is an involution. Clearly $x_r^{m_r} \in C_G(i)$, whence only finitely many of the $x_r^{m_r}$ are distinct. Consequently for some r the involution $x_r^{m_r}$ is centralized by infinitely many x_s. But this contradicts our assumption that the theorem is false.

Choose and fix an i-element $a \neq 1$ of odd order and write $k = ia$: then $k^2 = iaia = i^2a^ia = 1$. Since a cannot equal i, the element k is an involution.

(iii) *There exist infinitely many nontrivial i-elements b with odd order such that $u = ik^b$ is an i-element of odd order.* (Write S for the set of all such elements b.) In the first place u is an i-element because $u^i = k^bi = u^{-1}$. Next, since we are assuming that the theorem is false, $C_G(k)$ is finite, k being an involution. Hence, if b is allowed to vary over distinct right cosets of $C_G(k)$, we shall obtain infinitely many distinct elements of the form $u = ik^b$. An infinite number of these will have odd order by (ii).

The group $\langle i, k\rangle$ is a dihedral group in which $a = ik$ has odd order. Therefore $\langle i\rangle$ and $\langle k\rangle$ are conjugate, being Sylow 2-subgroups of $\langle i, k\rangle$. It follows that $i = k^{a_1}$ for some a_1 in $\langle a\rangle$.

(iv) *To each b in S there corresponds an h in $C_0(k)$ such that the involution $j = bi$ conjugates ha_1 to its inverse.* Let $u = ik^b$ be as in (iii). Since u has odd order, i and k^b are conjugate in $\langle i, k^b\rangle$, just as above; hence $i = (b^k)^{u_1}$ for some u_1 in $\langle u\rangle$. So we have $k^{bu_1} = i = k^{a_1}$, which implies that $h = bu_1a_1^{-1} \in C_G(k)$. Notice that $j = bi$ is an involution since $b^i = b^{-1}$. We now calculate $j^{-1}(ha_1)j = bibu_1bi = bb^iu_1^ib^i = bb^{-1}u_1^{-1}b^{-1} = u_1^{-1}b^{-1} = (ha_1)^{-1}$; keep in mind here that $b^i = b^{-1}$ and $u^i = u^{-1}$. This is what we wanted to prove.

(v) *Final step.* Using (iv) and the finiteness of $C_G(k)$, we can assert that there is an infinite subset T of S and an element h of $C_G(k)$ such that $j = bi$ conjugates $c = ha_1$ to its inverse for each b in T. Let b and b' be two ele-

ments of T; then $c^{bi} = c^{-1} = c^{b'i}$, so that $c^b = c^{b'}$ and $b(b')^{-1} \in C_G(c)$. Since T is infinite, we conclude that $C_G(c)$ is infinite.

Suppose that $c \in \zeta G$. Since $c = ha_1$ and $h \in C_G(k)$, it follows that $a_1 \in C_G(k)$. Hence $k = k^{a_1} = i$, which implies that $a = 1$, a contradiction. Consequently $c \notin \zeta G$, from which we see that $C_G(c)$ is a proper subgroup with nontrivial center. □

Before embarking on the proof of 14.3.7 we remark that use will be made of the solubility of groups of odd order. No proof is known which avoids using this difficult theorem of Feit and Thompson.

***Proof of* 14.3.7.** (i) *It is enough to prove that every infinite locally finite group has a nontrivial element with infinite centralizer.* Assume that this statement has been proved. Let G be an infinite locally finite group. Choose any finite abelian subgroup A_1 which has infinite centralizer C_1 in G—for example $A_1 = 1$ will do perfectly well. Then $A_1 \lhd C_1$ and C_1/A_1 is an infinite locally finite group. By hypothesis there is an element x of $C_1 \backslash A_1$ such that the centralizer $C_{C_1/A_1}(xA_1)$—let us call it D/A_1—is infinite. Since the subgroup $A_2 = \langle x, A_1 \rangle$ is finitely generated, it is finite; let $C_2 = C_G(A_2)$ and observe that $C_2 \leq D$; therefore $C_2 \leq C_D(x)$. On the other hand, $D \leq C_1$ implies that $C_D(x) \leq C_2$; thus $C_2 = C_D(x)$. Notice that $A_2 \lhd D$ because $[D, x] \leq A_1 \leq A_2$. It follows that

$$|D : C_D(x)| = |D : C_2| \leq |\text{Aut } A_2| < \infty.$$

Since D is infinite, we may conclude that $C_D(x)$ is infinite; consequently $C_G(A_2) = C_2$ is infinite.

By repeated application of this argument we are able to construct an infinite chain of finite abelian subgroups $A_1 < A_2 < \cdots$ such that each $C_G(A_i)$ is infinite. The union of the chain is an infinite abelian subgroup.

From now on it will be assumed that G is an infinite locally finite group such that every nontrivial element has finite centralizer. This will eventually lead to a contradiction.

(ii) *If F is a nontrivial finite subgroup of G, then $N_G(F)$ is finite.* For let $1 \neq x \in F$. Then $C_G(F) \leq C_G(x)$ and the latter is finite. Thus $C_G(F)$ is finite. By 1.6.13 we deduce that $N_G(F)$ is finite.

(iii) *There is a finite subgroup F such that $C_G(F) = 1$.* Let $1 \neq x \in G$: then $C_G(x)$ is finite, equal to $\{1, y_1, \ldots, y_n\}$ say, where $y_i \neq 1$. Since $C_G(y_i)$ is finite, we can pick z_i in G outside $C_G(y_i)$. Now put $F = \langle x, y_i, z_i | i = 1, \ldots, n \rangle$, surely a finite group. Clearly $C_G(F) \leq C_G(x)$; but since y_i and z_i do not commute, it follows that $C_G(F) = 1$.

(iv) *For each prime p the Sylow p-subgroups of G are finite and conjugate.* Suppose that P is an infinite Sylow p-subgroup. Since P is locally finite and nontrivial elements of P have finite centralizers, (iii) shows that $C_P(F) = 1$ for some finite subgroup F of P. But $\zeta F \leq C_P(F)$, so $\zeta F = 1$ and hence $F = 1$: this gives the contradiction $P = 1$. Conjugacy follows via 14.3.4.

(v) *Every proper quotient group of G is finite.* Let $1 \neq N \lhd G$. Then N has a nontrivial Sylow p-subgroup P for some prime p. Since Sylow p-subgroups of N are conjugate, the Frattini argument is available. Thus $G = N_G(P)N$ and $|G:N| = |N_G(P):N \cap N_G(P)|$, which is finite by (ii) and (iv).

(vi) *G is a locally soluble group without elements of order 2.* Šunkov's theorem (14.3.8) shows at once that G cannot contain an involution. Hence finitely generated subgroups of G have odd order and thus are soluble by the Feit–Thompson Theorem.

(vii) *G is not residually finite.* For suppose that G is residually finite. There is a nontrivial Sylow p-subgroup P of G for some prime p. Define

$$T = \langle C_G(x) | 1 \neq x \in P \rangle.$$

Since P is finite, T is a finite group. Moreover it is clear that $P \leq T$. By residual finiteness there is a normal subgroup K with finite index in G such that $K \cap T = 1$. Then $K \cap P = 1$. Since Sylow p-subgroups are conjugate, it follows that K has no elements of order p. Now $K \neq 1$, so there is a prime $q \neq p$ and a nontrivial Sylow q-subgroup Q of K. If $N = N_G(Q)$, the Frattini argument yields $G = NK$. Now $|P|$ divides $|G:K| = |N:N \cap K|$ since $P \simeq PK/K$. Hence Sylow p-subgroups of N have the same order as P and so are conjugate to P. Replacing P by a suitable conjugate—an operation that does not affect K since it is normal—we may suppose that $P \leq N$. Hence $Q^P = Q$.

The next step is to prove that PQ is a Frobenius group; it is, of course, finite. Let $1 \neq x \in P \cap P^y$ where $1 \neq y \in Q$. Then $x = a^y$ where $1 \neq a \in P$; therefore $[a, y] = a^{-1}x \in P \cap Q = 1$ since $Q \lhd PQ$. Hence $y \in K \cap C_G(a) \leq K \cap T = 1$ and $x = 1$. This shows that PQ is a Frobenius group. We now invoke 10.5.6 to conclude that the Frobenius complement P is cyclic, noting that p is odd.

It has just been proved that every Sylow subgroup of G is cyclic. It follows from 10.1.10 that finite subgroups of G are metabelian, which certainly causes G to be metabelian. If G were abelian and $1 \neq g \in G$, then $C_G(g) = G$ is finite. This is false, so $G' \neq 1$. Now let $1 \neq g \in G'$; then $G' \leq C_G(g)$, so G' is finite. Also G/G' is finite by (v), so again the contradiction that G is finite is attained.

(viii) *Conclusion.* Let R be the intersection of all the normal subgroups of finite index in G; then $R \neq 1$ by (vii). Hence G/R is finite by (v). Suppose that $1 \neq N \lhd R$. Now R is an infinite locally finite group with the finite centralizer property, just like G. Therefore (v) can be applied to show that R/N is finite. This makes $|G:N|$ finite, so the core of N has finite index in G. Hence this core contains R, which implies that $N = R$. Thus R is a simple group. However we have proved G to be locally soluble, whence so is R. A theorem of Mal'cev (12.5.2) now shows that R has prime order. Therefore G is finite, our final contradiction. □

We mention without proof two very important theorems about locally finite groups which have been proved in recent years.

I (Šunkov, Kegel–Wehrfritz). *A locally finite group whose abelian subgroups satisfy the minimal condition is a Černikov group.*

II (Šunkov). *Let G be a locally finite group and suppose that each abelian subgroup of G has finite rank. Then G is an extension of locally soluble group by a finite group (and has finite Prüfer rank in the sense of Exercise* 14.1.3).

For a detailed account of the theory of locally finite groups the reader is referred to [b18] and [b39].

Exercises 14.3

1. Show that in any group G there is a unique maximal normal locally finite subgroup R and that R contains all ascendant locally finite subgroups (see 12.1.4).
2. Prove 14.3.2.
3. (Baer). Show that in a Černikov group all Sylow p-subgroups are conjugate.
4. Let G be a countable locally finite group. If $N \lhd G$, show that every Sylow p-subgroup of G/N has the form PN/N where P is a Sylow p-subgroup of G.
5. Let G be a countable locally finite group with countably many Sylow p-subgroups. Show that in every quotient group of G all Sylow p-subgroups are conjugate.
6. (Kegel–Wehrfritz) Show that there is a countable metabelian, locally finite group with nonisomorphic Sylow p-subgroups by means of the following procedure.
   (a) Let p and q be distinct primes, let $X = \langle x \rangle$ have order q and $C = \langle c \rangle$ have order p. Let A be a group of type p^∞ with the usual generating set $\{a_1, a_2, \dots\}$. Define G to be the standard wreath product of $X \wr (A \times C)$. Show that $A \times C$ is a Sylow p-subgroup of G.
   (b) An element b_n of the base group of G is defined in the following way: the y-component of b_n is x if $y \in \langle a_n \rangle c$ and is otherwise 1. Put $u_n = a_n^{b_1 b_2 \cdots b_n}$. Show that $[a_{n-1}, b_n] = 1$ and that $u_n^p = u_{n-1}$, so that $U = \langle u_1, u_2, \dots \rangle$ is a group of type p^∞.
   (c) Let U be a contained in a Sylow p-subgroup P. If $U \neq P$, prove that $P \simeq A \times C$ and $G = BP$. Writing $c = b^{-1}v$ where $b \in B$, $v \in P$, obtain a contradiction. Conclude that U is a Sylow p-subgroup and $U \not\simeq A \times C$.
7. An infinite locally finite group of all whose proper subgroups are finite is quasicyclic.

*8. Without appeal to 14.3.7, prove that an infinite locally finite p-group G has an infinite abelian subgroup using the following argument.
   (a) Reduce to the case where G is countable. Assume that all abelian subgroups of G are finite.
   (b) If H is the hypercenter of G, prove that H is finite (using Exercise 12.2.4).
   (c) Show that every abelian subgroup of G/H is finite. Now assume that $H = 1$, so that $\zeta G = 1$.
   (d) Write $G = \bigcup_{i=1,2,\dots} G_i$ where $1 < G_1 \leq G_2 \leq \cdots$ and G_i is finite. Put $Z_i = \zeta G_i$ and show that $Z_i = Z_{i+1} =$ etc. for some i. Hence $Z_i \leq \zeta G$ and $\zeta G \neq 1$.

14.4. 2-Groups with the Maximal or Minimal Condition

For many years the following questions about groups with the maximal conditon (max) and the minimal condition (min) were outstanding.

(a) Is a group with max a finite extension of a soluble group?
(b) Is a group with min a finite extension of a soluble group?

Note that soluble groups with max or min are reasonably well understood —see 5.4.14 and 5.4.23. For example (b) would imply that a group with min is a Černikov group.

These conjectures have been verified in various special cases. For example (b) is true for locally finite groups by virtue of the Šunkov–Kegel–Wehrfritz theorem mentioned at the end of 14.3; trivially (a) is also true for this class of groups. In addition (b) has been proved for SN-groups (12.4.5).

However, recently Ol'šanskiĭ [a152] and Rips have constructed a number of remarkable examples which show that both conjectures are false in general. These include infinite groups all of whose proper nontrivial subgroups have prime order. Groups of this type are termed *Tarski groups.* Clearly they satisfy max and min and defeat both conjectures.

We shall now concentrate on 2-groups, showing that the two conjectures are true for such groups.

2-Groups with the Maximal Condition

Infinite 2-groups satisfy a weak form of the normalizer condition.

14.4.1. *If G is an infinite 2-group, each finite subgroup is properly contained in its normalizer in G.*

Proof. Suppose that F is a finite subgroup such that $F = N_G(F)$. Since G is infinite, not every finite subgroup is contained in F. Thus there is a finite subgroup M such that $I = M \cap F$ is maximal subject to $M \nleq F$. Now $I \neq N_M(I)$ because I is a proper subgroup of the nilpotent group M. Also $I < F$, from which it follows that $I < N_F(I)$. Consequently there exist elements of order 2 in $N_M(I)/I$ and $N_F(I)/I$, say xI and yI. Then $I^x = I = I^y$.

Let $T = \langle x, y, I \rangle$. Then $I \lhd T$ and T/I, being generated by two involutions, is a dihedral group. But T/I is also a 2-group, so it must be finite. It follows that T is finite. However this is impossible in view of the maximality of I; for $T \nleq F$ since $x \notin I$, and $I < T \cap F$ because $y \notin I$. □

Using this result one can quickly dispose of 2-groups with max.

14.4.2 (Kegel). *A 2-group which satisfies the maximal condition is finite.*

Proof. We assume that G is an infinite 2-group with max. Using 14.4.1 repeatedly, we can construct an infinite ascending chain of finite subgroups $F_1 < F_2 < \cdots$; for if F_i has been constructed, choose x_i from $N_G(F_i)\backslash F_i$ and define $F_{i+1} = \langle x_i, F_i \rangle = \langle x_i \rangle F_i$. Let U be the union of the chain; then U is obviously an infinite locally finite group, so by 14.3.7 it contains an infinite abelian subgroup V. (This use of the difficult theorem 14.3.7 can be avoided—see Exercise 14.3.8.) On the other hand, V is a finitely generated abelian 2-group, so it is finite. □

2-Groups with the Minimal Condition

14.4.3 (Schmidt). *A 2-group which satisfies the minimal condition is a Černikov group.*

Proof. (i) Let G be a 2-group with min. By 12.1.8 it is enough to prove that G is locally finite. Thus we shall assume this to be false and that G is minimal subject to not being locally finite. Then every proper subgroup of G is locally finite. It follows that the union of a chain of proper subgroups must be proper. Hence Zorn's Lemma implies that every proper subgroup lies in a maximal subgroup. Similarly a proper normal subgroup is contained in a maximal normal subgroup. If N is a maximal normal subgroup of G, then G/N cannot be locally finite by 14.3.1. Moreover G/N satisfies min and is a 2-group while all its proper subgroups are locally finite. In short G/N is as good as G, so let us suppose that $N = 1$ and G is simple.

(ii) *Each pair of distinct maximal subgroups intersects trivially.* Assume that this is false and let M and M_1 be maximal subgroups such that $I_1 = M \cap M_1 \neq 1$. In the ensuing proof it is understood that M is fixed. Since M_1 is a locally finite 2-group with min, it is hypercentral (12.2.5) and thus $I_1 < N_{M_1}(I_1)$ by 12.2.4. Now $Z_1 = \zeta I_1$ is characteristic in I_1 and thus normal in $N_{M_1}(I_1)$. Hence Z_1 is normalized by some element of $M_1 \backslash M$. Since $Z_1 \neq 1$ and G is simple, $N_G(Z_1)$ must be a proper subgroup of G; thus it is contained in a maximal subgroup M_2. Here $M_2 \neq M$ because $N_G(Z_1) \not\leq M$. Also $I_1 \leq N_M(Z_1) \leq M_2$, so that $I_1 \leq I_2 = M \cap M_2$.

By the minimal condition we may suppose that M_1 and M_2 have been chosen so that $N_G(Z_1) \leq M_2$ and $Z_2 = \zeta I_2$ is minimal. Just as above $N_G(I_2) < G$ and $N_G(Z_2) \not\leq M$. Therefore $N_G(Z_2)$ is contained in a maximal subgroup M_3 which cannot equal M. Now

$$I_1 \leq I_2 < N_M(I_2) \leq N_M(Z_2) \leq M \cap M_3 = I_3,$$

say. Consequently $Z_3 = \zeta I_3$ centralizes Z_1 and therefore $Z_3 \leq N_M(Z_1) \leq M \cap M_2 = I_2$, which in turn implies that $Z_3 \leq \zeta I_2 = Z_2$. Now the pair (M_2, M_3) has all the properties of the pair (M_1, M_2); since $Z_3 \leq Z_2$, the hypothesis of minimality leads to $Z_3 = Z_2$. It follows from this that

$$I_3 \leq N_M(Z_3) = N_M(Z_2) \leq M \cap M_3 = I_3;$$

hence $N_M(Z_2) = I_3$. However $I_3 < M$, which implies that some element of $M \backslash I_3$ normalizes I_3, and hence Z_3, a contradiction.

(iii) *Conclusion.* Let M and M_1 be two distinct maximal subgroups of G—these exist otherwise there is only one maximal subgroup which would then have to be normal. Let a and a_1 be involutions belonging to M and M_1 respectively. Then $A = \langle a, a_1 \rangle$ is finite because it is a dihedral group. Thus A is proper and is contained in a maximal subgroup M^*. But $1 \neq a \in M \cap M^*$ and $1 \neq a_1 \in M_1 \cap M^*$; thus (ii) shows that $M = M^* = M_1$, a contradiction. □

Exercises 14.4

1. Let G be a Tarski group, i.e., an infinite group all of whose proper nontrivial subgroups have prime order. Prove that G is a 2-generator simple group.
2. Show that there are no Tarski p-groups if $p < 5$.
3. Using the negative solution to the Burnside problem and the positive solution of the restricted Burnside problem (see 14.2), show that there is a finitely generated infinite simple group of exponent p where p is a large enough prime.
4. (Kegel). An infinite 2-group has an infinite abelian subgroup.

14.5. Finiteness Properties of Conjugates and Commutators

There are numerous finiteness properties which restrict in some way a set of conjugates or a set of commutators in a group. Sometimes these restrictions are strong enough to impose a recognizable structure on the group. We shall study finiteness properties of this type.

Finiteness Properties of the Upper and Lower Central Series

A basic theorem of Schur (10.1.4) asserts that if the center of a group G has finite index, then the derived subgroup of G is finite. Roughly speaking this says that if the center is large, the derived subgroup is small. This raises various questions: is there a generalization to higher terms of the upper and lower central series? Is there a converse? Theorems of Baer and P. Hall provide positive answers to these questions.

14.5.1 (Baer). *If G is a group such that $G/\zeta_i G$ is finite, then $\gamma_{i+1} G$ is finite.*

The case $i = 1$ is, of course, Schur's theorem. We shall deduce 14.5.1 from a lemma on commutator subgroups.

14.5.2 (Baer). *Let H, K, M, N be normal subgroups of a group G such that $M \leq N$ and $N \leq K$. Assume that $|H : M|$ and $|K : N|$ are finite, and also that $[H, N] = 1 = [K, M]$. Then $[H, K]$ is finite.*

Proof. Let $I = H \cap K$ and put $\bar{K} = K/C_K(I)$. Form the semidirect product $P = \bar{K} \ltimes I$, utilizing the action of $\bar{K}$ on I which arises from conjugation. Since $M \cap I$ is centralized by K, it is contained in the center of P. Now $I/M \cap I \simeq IM/M \leq H/M$, so $I/M \cap I$ is finite. Also $N \leq C_K(I)$ implies that $\bar{K}$ is finite. It follows that $P/M \cap I$, and hence $P/\zeta P$, is finite. We now infer from Schur's theorem that P' is finite; in particular $[\bar{K}, I] = [K, I]$ is finite. For similar reasons $[H, I]$ is finite. Hence $[H, I][K, I]$ is a finite normal subgroup contained in $[H, K]$. Evidently there is nothing to be lost in factoring out by this subgroup, so we assume that $[H, I] = 1 = [K, I]$. Since $[H, K] \leq I$ by normality of H and K, it follows that

$$[H, K, H] = 1 = [H, K, K]. \tag{8}$$

The Three Subgroup Lemma (5.1.10) can now be applied to yield $[H', K] = 1 = [H, K']$.

Consider the mapping $hH'M \otimes kK'N \mapsto [h, k]$ where $h \in H$ and $k \in K$; this is well-defined since $[H, K'N] = 1 = [H'M, K]$. It gives rise to a homomorphism from $(H/H'M) \otimes (K/K'N)$ onto $[H, K]$ by (8). But $H/H'M$ and $K[K'N$ are finite, whence so is their tensor product. Therefore $[H, K]$ is finite. □

***Proof of* 14.5.1.** We argue by induction on $i > 1$, the case $i \leq 1$ being known. Since $\zeta_{i-1}(G/\zeta G) = \zeta_i G/\zeta G$ has finite index in $G/\zeta G$, the induction hypothesis implies that $\gamma_i(G/\zeta G) = (\gamma_i G)\zeta G/\zeta G$ is finite. Apply 14.5.2 with $H = (\gamma_i G)\zeta G$, $M = \zeta G$, $K = G$, and $N = \zeta_i G$, noting that $[\gamma_i G, \zeta_i G] = 1$ by 5.1.11. The conclusion is that $[H, K] = \gamma_{i+1} G$ is finite. □

P. Hall has proved a partial converse of Baer's theorem.

14.5.3 (P. Hall). *If G is a group such that $\gamma_{i+1} G$ is finite, then $G/\zeta_{2i} G$ is finite.*

Combining 14.5.1 and 14.5.3 we can state that *some term of the upper central series has finite index if and only if some of the lower central series is finite.*

Theorem 14.5.3 requires a preliminary lemma on commutator subgroups.

14.5.4 (P. Hall). *Let G be a group and let $H = C_G(\gamma_{i+1} G)$. If l, m, n are integers satisfying $l + m + n \geq 2i - 1$, then $[[H, {}_l G], [H, {}_m G]] \leq \zeta_n G$.*

Proof. In the first place it is easy to prove by induction on n that

$$[[M, N], {}_nG] \leq \prod_{j+k=n} [[M, {}_jG], [N, {}_kG]]$$

whenever M and N are normal subgroups. Applying this with $M = [H, {}_lG]$ and $N = [H, {}_mG]$ we obtain

$$[[M, N], {}_nG] \leq \prod_{j+k=n} [[H, {}_{l+j}G], [H, {}_{m+k}G]].$$

Now $(l + j) + (m + k) = l + m + n \geq 2i - 1$, so that either $l + j \geq i$ or $m + k \geq i$. Hence either $[H, {}_{l+j}G] \leq \gamma_{i+1}G$ or $[H, {}_{m+k}G] \leq \gamma_{i+1}G$. But H centralizes $\gamma_{i+1}G$, so we conclude that $[[H, {}_{l+i}G], [H, {}_{m+k}G]] = 1$ in any event. Consequently $[M, N] \leq \zeta_n G$. □

***Proof of* 14.5.3.** Let $H = C_G(\gamma_{i+1}G)$. By hypothesis $\gamma_{i+1}G$ is finite, so $|G:H|$ is finite. Consider the factor

$$F_s = [H, {}_{i-s}G]/[H, {}_{i-s}G] \cap \zeta_{i+s}G,$$

where $0 \leq s \leq i$. We would like to prove that F_s is finite. Certainly F_0 is finite; for it is a factor of $\gamma_{i+1}G$. Assume that F_s is finite for some $s < i$.

By 14.5.4 we have

$$[[H, {}_{i-s}G], H] \leq \zeta_{i+s}G$$

because $(i - s) + 0 + (i + s) = 2i > 2i - 1$. Therefore F_s is a central factor of H. It follows that if g is a fixed element of G, the mapping

$$x \mapsto [x, g]([H, {}_{i-s}G] \cap \zeta_{i+s}G)$$

is a homomorphism from $L = [H, {}_{i-s-1}G]$ into the finite group F_s. Then $L/K(g)$ is finite where $K(g)$ is the kernel of the homomorphism.

Choose a transversal $\{t_1, \ldots, t_r\}$ to H in G and let

$$K = K(t_1) \cap \cdots \cap K(t_r).$$

Then L/K is finite. The definition of $K(t_i)$ shows that $[K, t_i] \leq [K(t_i), t_i] \leq \zeta_{i+s}G$. Also $[K, H] \leq [L, H] \leq \zeta_{i+s}G$ by 14.5.4. Since $G = \bigcup_{i=1}^{r} Ht_i$, it follows that $[K, G] \leq \zeta_{i+s}G$ and $K \leq \zeta_{i+s+1}G$. Hence $K \leq L \cap \zeta_{i+s+1}G$, which shows that $F_{s+1} = L/L \cap \zeta_{i+s+1}G$ is finite.

Thus F_s is finite for all s. Taking $s = i$ we conclude that $H/H \cap \zeta_{2i}G$ is finite, so that $\zeta_{2i}G$ has finite index in $H\zeta_{2i}G$. Since $|G:H|$ is finite, the result follows. □

Groups with Finite Conjugacy Classes

An element g of a group G is called an *FC-element* if it has only a finite number of conjugates in G, that is to say, if $|G: C_G(g)|$ is finite. It is a basic fact that the FC-elements always form a subgroup.

14.5.5 (Baer). *In any group G the FC-elements form a characteristic subgroup.*

Proof. Let g and h be FC-elements of G. Then $C_G(g)$ and $C_G(h)$ have finite index, which implies that $C_G(g) \cap C_G(h)$ has finite index. But obviously $C_G(gh^{-1}) \geq C_G(g) \cap C_G(h)$, so $C_G(gh^{-1})$ has finite index and gh^{-1} is an FC-element. Thus the FC-elements form a subgroup. If $\alpha \in \text{Aut}\, G$, then $C_G(g^\alpha) = C_G(g)^\alpha$, from which it follows that $C_G(g^\alpha)$ has finite index. Hence g^α is an FC-element. □

An FC-element may be thought of as a generalization of an element of the center of the group; for elements of the latter type have just one conjugate. For this reason the subgroup of all FC-elements is called the *FC-center*: of course it always contains the center.

A group G is called an *FC-group* if it equals its FC-center, which amounts to saying that every conjugacy class of G is finite. Prominent among the FC-groups are groups with center of finite index: in such a group each centralizer must be of finite index because it contains the center. Of course in particular all abelian groups and all finite groups are FC-groups.

It is very easy to see that the class of FC-groups is closed with respect to forming subgroups, images and direct products—as the reader should verify.

The following result draws attention to FC-groups that are torsion groups.

14.5.6 (Baer). *If G is an FC-group, then $G/\zeta G$ is a residually finite torsion group.*

Proof. ζG is the intersection of all the centralizers of elements of G. Since each of the latter has finite index, $G/\zeta G$ is surely residually finite.

To see that $G/\zeta G$ is a torsion group take any x in G and choose a right transversal $\{t_1, \dots, t_k\}$ to $C_G(x)$ in G. Then $C_G(t_1) \cap \cdots \cap C_G(t_k)$ has finite index in G, whence so does its core K. Thus $x^m \in K$ for some positive integer m. It follows that x^m centralizes each t_i. But the t_i and $C_G(x)$ generate G; therefore $x^m \in \zeta G$. □

In the study of FC-groups that are torsion groups the following simple lemma is invaluable. Herein a subset of a group will be termed *normal* if it contains all conjugates of its elements.

14.5.7 (Dicman's Lemma). *In any group G a finite normal subset consisting of elements of finite order generates a finite normal subgroup.*

Proof. Let $X = \{x_1, x_2, \dots, x_n\}$ be the normal subset and let $H = \langle X \rangle$. Obviously H is normal in G: we have to prove that it is finite.

If $1 \neq h \in H$, then $h = x_{\alpha_1}^{m_1} \cdots x_{\alpha_r}^{m_r}$ where $1 \leq \alpha_i \leq n$. In general there will be many such expressions for h, among them some of shortest length, say r. Furthermore among these expressions of shortest length there is one which

appears first in the lexicographic ordering of r-tuples: this is the ordering in which $(\alpha_1, \ldots, \alpha_r)$ precedes $(\alpha'_1, \ldots, \alpha'_r)$ if $\alpha_i = \alpha'_i$ for $i < s$ and $\alpha_s < \alpha'_s$ for some $s \leq r$. Denote this first expression by $h = y_1 y_2 \cdots y_r$ where $y_i = x_{\alpha_i}^{m_i}$.

Suppose that $\alpha_i = \alpha_j$ where $i < j$. Moving y_j to the left we obtain

$$h = y_1 \cdots y_{i-1}(y_i y_j) y_{j+1}^{y_j} \cdots y_{j-1}^{y_j} y_{j+1} \cdots y_r,$$

an expression of length less than r. Consequently the α_i are all different.

Now assume that $\alpha_i > \alpha_{i+1}$; then

$$h = y_1 \cdots y_{i-1} y_{i+1} y_i^{y_{i+1}} y_{i+2} \cdots y_r.$$

But this expression of length r precedes $y_1 y_2 \cdots y_r$ in the ordering of r-tuples. Hence $\alpha_1 < \alpha_2 < \cdots < \alpha_r$. It follows that there are at most $\prod_{i=1}^n |x_i|$ possibilities for h. □

This allows us to describe FC-torsion groups in a different manner.

14.5.8. *A torsion group G is an FC-group if and only if each finite subset is contained in a finite normal subgroup.*

Proof. Let G be an FC-group and let F be a finite subset of G. The set of conjugates of elements of F in G is a finite normal subset. By 14.5.7 it generates a finite normal subgroup. Conversely, if G has the property in question and $x \in G$, then $x \in F \lhd G$ for some finite F. All conjugates of x belong to F, so there are only finitely many of them. □

Groups with the property of 14.5.8 are often called *locally finite and normal groups* instead of torsion FC-groups. Notable examples are direct products of finite groups, their subgroups and quotient groups.

Returning to general FC-groups we shall use Schur's theorem to establish a basic fact about the commutator subgroup of an FC-group.

14.5.9 (B.H. Neumann). *If G is an FC-group, then G' is a torsion group. Also the elements of finite order in G form a fully-invariant subgroup containing G'.*

Proof. By 14.5.6 and 14.5.8 the group $G/\zeta G$ is locally finite. Now if X is a finitely generated subgroup of G, then $X/X \cap \zeta G$ is finite, which implies that $X/\zeta X$ is finite. Hence X' is finite by Schur's theorem. Obviously G' is the union of all such X', so G' is a torsion group. Next let x, y in G satisfy $x^m = 1 = y^n$ where $m, n > 0$. Then $(xy^{-1})^{mn} \equiv 1 \bmod G'$. Therefore $(xy^{-1})^l = 1$ for some $l > 0$. Hence the elements of finite order form a subgroup containing G'. □

We have discovered enough about FC-groups to be able to characterize them in terms of torsion-free abelian groups and locally finite and normal groups.

14.5.10. *A group G is an FC-group if and only if it is isomorphic with a subgroup of the direct product of a torsion-free abelian group and a locally finite and normal group.*

Proof. Suppose that G is an FC-group and let T be the set of elements of finite order. Then $G' \leq T \leq G$ by 14.5.9, so that G/T is a torsion-free abelian group. By Zorn's Lemma there exists a maximal torsion-free subgroup of the center—call it M. Then it is easy to see that $\zeta G/M$ is a torsion group. But $G/\zeta G$ is a torsion group by 14.5.6; hence G/M is a torsion group. Since G/M is clearly an FC-group, it is locally finite and normal. Now $T \cap M = 1$ because T is torsion and M is torsion-free. Consequently the mapping $x \mapsto (xT, xM)$ is an embedding of G in $(G/T) \times (G/M)$.

The converse follows from the fact that the class of FC-groups is closed with respect to forming subgroups and direct products. □

Since it is not easy to describe the subgroups of a direct product, 14.5.10 does not provide a completely satisfactory classification of FC-groups.

Groups with Boundedly Finite Conjugacy Classes

A group G is called a *BFC-group* if there is a positive integer d such that no element of G has more than d conjugates. BFC-groups form a very special class of FC-groups which admits a precise description.

14.5.11 (B.H. Neumann). *A group G is a BFC-group if and only if the commutator subgroup G' is finite.*

Proof. If G' has finite order d, then the number of commutators $[g, x]$ cannot exceed d. Hence the number of conjugates of an element g is at most equal to d. Thus G is a BFC-group.

Conversely let G be a BFC-group; denote by d the maximum number of elements in a conjugacy class. Then there is an element a with exactly d conjugates in G; thus $|G : C_G(a)| = d$. Choose a right transversal $t_1, \dots, t_d$ to $C_G(a)$; then $a^{t_1}, \dots, a^{t_d}$ are the d distinct conjugates of a. Define C to be the intersection of the centralizers $C_G(t_i)$, $i = 1, \dots, d$. Since $|G : C|$ is finite, there is a finite right transversal $\{s_1, \dots, s_k\}$ to C in G.

Now consider

$$N = \langle a, s_1, \dots, s_k \rangle^G.$$

This is a finitely generated FC-group, so its center has finite index by 14.5.6 and 14.5.8. Schur's theorem shows that the elements of finite order in N form a finite subgroup. Since G' is a torsion group (14.5.9), it is sufficient to prove that $G' \leq N$.

If $x \in C$, then $(xa)^{t_i} = xa^{t_i}$ since $C \leq C_G(t_i)$. From this it is apparent that the d elements xa^{t_i} are distinct and account for all the conjugates of xa in G. Consequently, if $y \in C$, there is an i such that $(xa)^y = xa^{t_i}$; this implies that $x^y = xa^{t_i}a^{-y}$ and $[x, y] = a^{t_i}a^{-y} \in N$. Hence $C' \leq N$. But $G = NC$ implies that $G' \leq NC' \leq N$. □

Subgroups of Direct Products of Finite Groups

It has been observed that any subgroup of a direct product of finite groups is locally finite and normal. Are such subgroups typical of locally finite and normal groups? Since a direct product of finite groups is residually finite, only locally finite and normal groups with the latter property can arise as subgroups. Precisely what further conditions the locally finite and normal group must satisfy is unknown. For countable groups however the situation is well understood.

14.5.12 (P. Hall). *A countable locally finite and normal group G is isomorphic with a subgroup of a direct product of finite groups if and only if it is residually finite.*

Proof. Only the sufficiency of this condition is in doubt. Assume therefore that G is residually finite and let $G = \{g_1, g_2, \dots\}$. Writing G_i for the normal closure of $\{g_1, g_2, \dots, g_i\}$, we obtain G as the union of an ascending chain of finite normal subgroups $1 = G_0 \leq G_1 \leq G_2 \leq \cdots$.

Let us show how to construct a descending chain of normal subgroups of finite index $G = R_1 \geq R_2 \geq \cdots$ such that $G_i \cap R_i = 1$. Suppose that R_i has already been chosen. Since G is residually finite, there is a normal subgroup N of finite index such that $N \cap G_{i+1} = 1$. Define $R_{i+1} = N \cap R_i$, clearly a normal subgroup of finite index; then

$$G_{i+1} \cap R_{i+1} = (G_{i+1} \cap N) \cap R_i = 1.$$

Thus the construction has been effected.

Define S_{i+1} to be $G_i R_{i+1}$, $i = 0, 1, \dots$, again a normal subgroup with finite index in G. Then

$$G_{i+1} \cap S_{i+1} = G_{i+1} \cap (G_i R_{i+1}) = G_i(G_{i+1} \cap R_{i+1}) = G_i. \tag{9}$$

Now given $g \neq 1$ in G, there is an i such that $g \in G_{i+1} \backslash G_i$; hence $g \notin S_{i+1}$ by (9). It follows that the intersection of all the S_i is 1. In addition, a given element g of G belongs to almost all of the G_i and therefore to almost all of the S_i. This means that the mapping $g \mapsto (S_1 g, S_2 g, \dots)$ is a homomorphism from G into the *direct product*, not merely the cartesian product, of the G/S_i. It is also injective because $S_1 \cap S_2 \cap \cdots = 1$. Thus the theorem is proved. □

For information about the uncountable case see [b69], which is a good general reference for FC-groups.

Groups with Finitely Many Elements of Each Order

As the last topic of the chapter we consider groups that possess only a finite number of elements of each order, including ∞. We shall call these *FO-groups*—they are sometimes known as groups with finite layers. Notice that an FO-group is an FC-group: for conjugate elements have the same order. So we are confronted with a special type of FC-group—so special in fact that a satisfactory structural description is possible.

First a couple of elementary results.

14.5.13 (Baer). (i) *An FO-group is locally finite and normal.*

(ii) *Every Černikov group whose centre has finite index is an FO-group.*

Proof. (i) If a group has an element of infinite order, it has an infinity of such elements. An FO-group is therefore a torsion group, so by 14.5.8 it is locally finite and normal.

(ii) Let G be a Černikov group whose center C has finite index; of course G is a torsion group. Choose a transversal $\{t_1, \dots, t_k\}$ to C in G and let t_i have order m_i. Let us consider elements of G which have some fixed order m. If g has order m and $g = ct_i$, $(c \in C)$, then $1 = (ct_i)^m = c^m t_i^m$. Hence $c^{mm_i} = 1$. Now C has only a finite number of elements of order dividing mm_i by 4.2.11. Consequently there are only finitely many possibilities for g and G is an FO-group. □

We come now to the main theorem on FO-groups from which most properties of these groups can be read off. In essence it says that all FO-groups arise as subgroups of certain direct products of Černikov groups with center of finite index. Thus groups of the latter type may be regarded as prototypes of FO-groups.

In the next theorem a direct product will be called *prime-sparse* if for each prime p only a finite number of the direct factors possess elements of order p.

14.5.14 (Černikov, Polovickiĭ). *The following statements about a group G are equivalent.*

(i) *G is an FO-group.*
(ii) *G is locally finite and normal and each Sylow subgroup is a Černikov group.*
(iii) *G is isomorphic with a subgroup of a prime-sparse direct product of Černikov groups with centers of finite index.*

Proof. (i) $\rightarrow$ (ii). Let G be an FO-group; then G is locally finite and normal by 14.5.13. Consider a Sylow p-subgroup P of G and let R be generated by all subgroups of P which have no proper subgroups of finite index. Then $R \leq P$ and it is easy to see that R itself has no proper subgroups of finite index. Also if $R < S \leq G$, then S/R must have a proper subgroup with finite index. If $g \in P$, then $|R : C_R(g)|$ is finite since R is an FC-group. It follows that $R = C_R(g)$ and $R \leq \zeta P$. Thus R is a divisible abelian p-group.

Next, Exercise 4.3.5 shows that abelian subgroups of P have min; thus R has min. We claim that P/R is also an FO-group. To see this consider an element xR of P/R with order m. Then $x^m \in R$ and $x^m = y^m$ for some $y \in R$ because R is divisible. Hence $(xy^{-1})^m = 1$ since $R \leq \zeta P$. It follows that there are only finitely many possibilities for xy^{-1} and thus for xN. We conclude that abelian subgroups of P/R have min. The structure of groups with min and the maximality of R shows that abelian subgroups of P/R are actually finite. By Exercise 14.3.8 the group P/R is finite. Thus P is a Černikov group and $P/\zeta P$ is finite.

(ii) $\rightarrow$ (iii). This is the main point of the proof. We shall prove it in four steps. Let G satisfy (ii).

(a) *The p-elements of G generate a Černikov subgroup.* Since G is an FC-group, a subgroup of type p^∞ is contained in the center of G. Hence the p^∞-subgroups generate a subgroup R of the center. Clearly R is a divisible abelian p-group. Let P be any Sylow p-subgroup of G. Then $R \leq P$ since $R \lhd G$. Since, by hypothesis, P is a Černikov group, it has a divisible abelian subgroup of finite index which must equal R. Thus $\bar{P} = P/R$ is finite. It is clear that $\bar{P}$ is a Sylow p-subgroup of $\bar{G} = G/R$. Thus 14.3.4 shows that each Sylow p-subgroup of $\bar{G}$ is conjugate to $\bar{P}$ and thus is contained in $\bar{P}^{\bar{G}}$. But $\bar{P}^{\bar{G}}$ is finite because $\bar{G}$ is locally finite and normal; thus we have proved that the p-elements of $\bar{G}$ generate a finite subgroup. Since R satisfies min, the assertion (a) is true.

(b) *In every image of G the p-elements generate a Černikov subgroup.* Let $N \lhd G$ and let gN be a p-element of G/N. Then g has order lp^m where $g^{p^m} \in N$ and l is a positive integer coprime to p. Now $al + bp^m = 1$ for suitable integers a and b. Hence we have $g = g^{al}g^{bp^m} \equiv g^{al} \bmod N$. Here g^{al} is a p-element, so we may as well assume in the first place that g is a p-element. Consequently the p-elements of G/N generate a subgroup SN/N where S is generated by all p-elements of G. The assertion now follows from (a).

(c) *If M is the maximum normal p'-subgroup of G, then G/M is a Černikov group.* By (b) the quotient group G/M inherits the properties of G. So without loss of generality assume that $M = 1$. According to (a) the p-elements of G generate a Černikov group T. Now a quasicyclic subgroup of G lies in the center and must be a p-group since $M = 1$. Hence the quasicyclic subgroups of G generate a p-subgroup S contained in $T \cap (\zeta G)$. Next $G/C_G(T/S)$ must be finite because T/S is finite. Furthermore, if $x \in C_G(T/S)$, the mapping $yS \mapsto [x, y]$ is a well-defined homomorphism x^θ from T/S to S; also $\theta\colon C_G(T/S) \rightarrow L \equiv \mathrm{Hom}(T/S, S)$ is a homomorphism. Here it is essential to

observe that $S \leq \zeta G$. Now L is finite since T/S is finite and S has only a finite number of elements of each given order. Consequently $C_G(T/S)/\text{Ker}\ \theta$ is finite. Clearly $\text{Ker}\ \theta = C_G(T) = K$, say. Thus G/K is finite.

It remains to prove that K is a Černikov group. The p-elements of K belong to $T \cap K$, so that $K/\zeta K$ is a p'-group. By Exercise 10.1.3 the p'-elements of K form a fully-invariant subgroup of K, which will be normal in G. But G has no nontrivial normal p'-subgroups. Hence K is a p-group and $K \leq T$, which shows that K is a Černikov group.

(d) *Conclusion.* Let $p_1, p_2, \ldots$ be the sequence of primes and let M_i be the maximum normal p_i'-subgroup of G. By (c) we know that G/M_i is a Černikov group: this group is also locally finite and normal (since G is), so all quasicyclic subgroups of G/M_i are central and the center of G/M_i has finite index. Clearly the intersection of all the M_i is 1, so that the mapping $g \mapsto (gM_1, gM_2, \ldots)$ is a monomorphism into the cartesian product of the G/M_i. We shall prove that the image of this mapping is contained in the direct product of the G/M_i.

Let p be any prime. Then the p-elements of G generate a Černikov group P by (a). Naturally the prime divisors of the orders of elements of P constitute a finite set of primes π. If $p_i \notin \pi$, then P is a normal p_i'-subgroup and $P \leq M_i$. So only a finite number of the groups G/M_i contain an element of order p. It follows that an element of finite order in the cartesian product of the G/M_i must belong to the direct product; moreover the latter is prime-sparse. Hence the image of G is contained in the direct product of the G/M_i.

(iii) → (i). The elements of order m are contained in the product of finitely many direct factors and hence in a Černikov group whose centre has finite index. The implication follows via 14.5.13. □

14.5.15. *An image of an FO-group is an FO-group.*

Proof. Let $N \lhd G$ where G is an FO-group. Then G/N is certainly locally finite and normal. Let P/N be a Sylow p-subgroup. Then it is easy to see that P can be generated by N together with p-elements. But the p-elements of G generate a Černikov group by 14.5.14 (or more simply by (a) of the second implication in the proof), so P/N too has this structure. Applying 14.5.14 we conclude that G/N is an FO-group. □

Notice that 14.5.15 does not follow in an obvious way from the definition of an FO-group.

Exercises 14.5

1. A group G is FC if and only if $G/C_G(x^G)$ is finite for every x in G.
2. (B.H. Neumann). A finitely generated group is FC if and only if it is a finite extension of its center (hence such groups have max).

3. A group with min-n in FC if and only if it is a Černikov group whose center has finite index (hence such groups have min). Find a similar characterization of FC-groups with max-n.

4. A direct product of FC-groups is an FC-group. But a group that is a product of two normal FC-subgroups need not be an FC-group. [*Hint*: A free nilpotent group with class and rank equal to 2.]

5. (Fedorov). Prove that the only infinite group all of whose proper subgroups have finite index is the infinite cyclic group.

6. (McLain). A locally nilpotent FC-group is hyercentral. [*Hint*: If $G \neq 1$ is such a group, find a nontrivial normal subgroup N which is free or elementary abelian with finite rank. Consider the action of G on N and apply 8.1.10.]

7. If G is a finitely generated group such that $\gamma_{i+1}G$ is finite, prove the $G/\zeta_i G$ is finite. Show that this is not true for nonfinitely generated groups. [*Hint*: Use induction on i. Let $C = C_G(\gamma_{i+1}G)$ and consider the map $C \cap \gamma_i G \to \gamma_{i+1}G$ given by $x \mapsto [x, g]$ where g is a generator.]

8. (P. Hall). Every countable residually finite, locally finite and normal group is isomorphic with a subgroup of $S_2 \times S_3 \times S_4 \times \cdots$.

9. (Černikov). The following properties of a group G are equivalent:
   (a) G is torsion and for each prime p the group has only finitely many p-elements;
   (b) G is locally finite and normal and all Sylow subgroups are finite;
   (c) G is isomorphic with a subgroup of a prime-sparse direct product of finite groups.

10. (Černikov). A group with the properties of Exercise 14.5.9 need not be a direct product of finite groups. Proceed as follows.
    (a) Choose distinct primes $p_1, p_2, \ldots$ such that $p_{2i} \equiv 1 \bmod(p_{2i+1}p_{2i-1})$.
    (b) Let $\langle x_i \rangle$ have order p_i and put $X = \langle x_1 \rangle \times \langle x_3 \rangle \times \cdots$ and $Y = \langle x_2 \rangle \times \langle x_4 \rangle \times \cdots$. Since p_{2i+1} divides $p_{2i} - 1$ and $p_{2i+2} - 1$, there is a natural action of x_{2i+1} on $\langle x_{2i} \rangle$ and $\langle x_{2i+2} \rangle$. Use this to construct an action of X on Y and put $G = X \ltimes Y$.
    (c) Prove that G is locally finite and normal and has finite Sylow subgroups.
    (d) Prove that G is directly indecomposable.

11. (Schenkman). Let G be a locally finite group.
    (a) Prove that G has finitely many Sylow p-subgroups if and only if $G/O_p(G)$ is an extension of a finite group by a p'-group. [*Hint*: If $P_1, \ldots, P_k$ are the finitely many Sylow p-subgroups of G, consider $D = \bigcap_{i=1}^k N_G(P_i)$.]
    (b) Let H be the Hirsch–Plotkin radical of G. Show that if G has finitely many Sylow p-subgroups for each prime p, then G/H has the structure given in Exercise 14.5.9.

CHAPTER 15

Infinite Soluble Groups

The theory of infinite soluble groups has developed in directions quite different from the older theory of finite soluble groups. A noticeable feature of the infinite theory is the strong interaction with commutative algebra, which is due to the role played by the group ring. Despite this fact the exposition that follows is largely self-contained.

15.1. Soluble Linear Groups

If R is a ring with identity, we say that a group G is *R-linear* (or simply *linear* if the ring is understood) if it is isomorphic with a subgroup of the matrix group $\mathrm{GL}(n, R)$ for some positive integer n. Equivalently one could say that G is isomorphic with a group of R-automorphisms of a finitely generated free R-module. Our interest will center on two cases, where R is a field or the ring of integers.

It is natural to ask which groups are linear. Rather obviously a finite group G is R-linear for every R: for we can use the regular representation to identify G with a group of permutation matrices over R. It follows that linearity is a finiteness condition in the sense of 14.1.

In 2.1 we observed that the matrices

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

generate a free group of rank 2: taking the derived subgroup and applying 6.1.7 we conclude that *every countable free group is $\mathbb{Z}$-linear*. On the other hand, there exist infinite groups which are not linear over any field, as we shall see in 15.1.5.

The intrusion of linear groups into the theory of soluble groups is easily explained. Suppose that G is a soluble group with a normal abelian subgroup A. Then $\bar{G} = G/C_G(A)$ is isomorphic with a group of automorphisms of A. If A is an elementary abelian p-group of finite rank n, then $\operatorname{Aut} A \simeq \operatorname{GL}(n, p)$, so $\bar{G}$ is linear over the field of p elements. If A is free abelian of rank n, then $\operatorname{Aut} A \simeq \operatorname{GL}(n, \mathbb{Z})$ and $\bar{G}$ is $\mathbb{Z}$-linear.

Finally, suppose that A is a torsion-free abelian group of finite rank n. Let $V = A \otimes_{\mathbb{Z}} \mathbb{Q}$, which is a rational vector space of dimension n. Then V becomes a $\bar{G}$-module via the natural action $(a \otimes r)\bar{g} = a^{g} \otimes r$. In this case $\bar{G}$ is isomorphic with a subgroup of $\operatorname{GL}(n, \mathbb{Q})$ and $\bar{G}$ is $\mathbb{Q}$-linear.

It is apparent from these examples that information about the structure of soluble linear groups is likely to be useful in the study of soluble groups whose abelian factors have finite p-rank for $p = 0$ or a prime.

The Lie–Kolchin–Mal'cev Theorem

Let V be a vector space of dimension n over a field F. A subgroup G of $\operatorname{GL}(V)$ is called *triangularizable* if it is possible to find a basis for V with respect to which G is represented by a group of (upper) triangular matrices. We saw in 5.1 that the group $T(n, F)$ of all triangular matrices is soluble. Thus every triangularizable subgroup is soluble.

In the same spirit a subgroup of $\operatorname{GL}(V)$ is called *diagonalizable* if it can be represented by a group of diagonal matrices by means of a suitable choice of basis. Diagonalizable subgroups are, of course, abelian.

The main result of this section may be regarded as a partial converse to the statements of the last two paragraphs. The final version, due to Mal'cev, improves earlier results of Lie and Kolchin.

15.1.1 (Lie, Kolchin, Mal'cev). *Let V be a vector space of dimension n over an algebraically closed field F. Suppose that G is a soluble subgroup of* $\operatorname{GL}(V)$.

(i) *If G is irreducible, there is a normal diagonalizable subgroup D with finite index not exceeding $g(n)$ for some function g.*
(ii) *In general there is a normal triangularizable subgroup T with finite index not exceeding $h(n)$ for some function h.*

The key to this important result is the special case when G is irreducible and *primitive*. Here a subgroup G of $\operatorname{GL}(V)$ is said to be primitive if there does *not* exist a decomposition

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k, \qquad (k > 1),$$

into nonzero F-subspaces such that elements of G permute the V_i.

15.1.2 (Zassenhaus). *Let V be as in* 15.1.1 *and suppose G is a primitive irreducible soluble subgroup of* $\operatorname{GL}(V)$. *Then there is a normal subgroup S con-*

sisting of scalar transformations such that $|G:S| \le n^2 f(n^2)$ where $f(m)$ is the maximum number of automorphisms of an abelian group of order m or less.

Proof. Let A be a normal abelian subgroup of G. Since G is irreducible, V is a simple FG-module with the natural action of G on V. By Clifford's Theorem (8.1.3) we can write $V = V_1 \oplus \cdots \oplus V_k$ where the V_i are the so-called *homogeneous components*, direct sums of isomorphic simple FA-modules; moreover elements of G permute the V_i. Since G is primitive, $k = 1$ and $V = V_1$. Because F is algebraically closed and A is abelian, a simple FA-module has dimension 1—this is by 8.1.6. It follows that A consists of scalar multiplications; in particular A is contained in C, the centre of G. Thus every normal abelian subgroup of G is contained in C and is scalar.

The remainder of the proof is concerned with a maximal normal abelian subgroup B/C of G/C, the object being to prove that

$$|B:C| \le n^2 \qquad \text{and} \qquad C_G(B/C) = B.$$

Once this has been achieved we shall be able to conclude that

$$|G:B| = |G:C_G(B/C)| \le |\mathrm{Aut}(B/C)| \le f(n^2)$$

by definition of f. Hence $|G:C| \le n^2 f(n^2)$ as required.

To begin with suppose that $C_G(B) \not\le C$. Then $C_G(B)/C$, being normal, must contain a nontrivial normal abelian subgroup of G/C, say D/C. Now BD/C is abelian because $[B, D] = 1$, so the maximality of B/C leads us to $D \le B$. Hence $D \le \zeta B$ and D is abelian. By the first paragraph $D = C$, which is a contradiction. Thus we have proved that $C_G(B) = C$.

Next let $\{b_1, \dots, b_r\}$ be a finite subset of a transversal to C in B. Suppose that this subset is linearly dependent (in the vector space $\mathrm{End}_F(V)$). After relabelling the b_i's if necessary, we can find a relation of the form $\sum_{i=1}^{s} f_i b_i = 0$ where $0 \ne f_i \in F$ and the length s is minimal. Now $b_1 b_2^{-1} \notin C = C_G(B)$. Hence $[b_1 b_2^{-1}, x] \ne 1$ for some x in B. This implies that $[b_1, x] \ne [b_2, x]$. Now, since $[b_i, x] \in C$, we can write $[b_i, x] = t_i 1$ with $t_i \in F$—recall that C is scalar. Then $t_1 \ne t_2$ and, since $x^{-1} b_i x = b_i [b_i, x] = t_i b_i$,

$$\begin{aligned} 0 &= t_1\left(\sum_{i=1}^{s} f_i b_i\right) - x^{-1}\left(\sum_{i=1}^{s} f_i b_i\right)x \\ &= t_1\left(\sum_{i=1}^{s} f_i b_i\right) - \sum_{i=1}^{s} f_i t_i b_i \\ &= \sum_{i=2}^{s} (t_1 - t_i) f_i b_i. \end{aligned}$$

But s was chosen minimal, so $(t_1 - t_2)f_2 = 0$ and $f_2 = 0$, a contradiction. It follows that $\{b_1, \dots, b_r\}$ is linearly independent in $\mathrm{End}_F(V)$. Since the latter has dimension n^2, we obtain $|B:C| \le n^2$.

It must still be shown that $K \equiv C_G(B/C)$ equals B. Of course $B \le K$ because B/C is abelian. If $k \in K$, the map θ_k which sends bC to $[b, k]$ is

plainly a homomorphism from B/C to C. What is more, the assignment $k \mapsto \theta_k$ is a homomorphism from K to $\mathrm{Hom}(B/C, C)$ whose kernel is precisely $C_K(B)$, that is, C. Thus K/C is isomorphic with a subgroup of $\mathrm{Hom}(B/C, C)$. Since C is scalar, it is isomorphic with a subgroup of F^*, the multiplicative group of F. But finite subgroups of F^* are cyclic, so the order of $\mathrm{Hom}(B/C, C)$ cannot exceed that of $H = \mathrm{Hom}(B/C, \mathbb{Z}_m)$ where $m = |B:C|$. Thus $|K:C| \leq |H| = |B:C|$. Finally $B \leq K$, so $|B:C| \leq |K:C|$. It follows that $B = K$. □

***Proof of* 15.1.1.** (i) Here G is assumed irreducible. By 15.1.2 we can also assume that G is not primitive, so there is a decomposition $V = V_1 \oplus \cdots \oplus V_k$ where $n \geq k > 1$ and the nonzero subspaces V_i are permuted transitively by the elements of G. If $g \in G$, then $V_i g = V_{(i)\pi_g}$ where $\pi_g \in S_k$. Now $g \mapsto \pi_g$ is a homomorphism from G to the symmetric group S_k whose kernel K is the intersection of all the subgroups $K_i = \{g \in G \mid V_i g = V_i\}$. Thus $|G:K| \leq k! \leq n!$.

Consider the FK_i-module V_i; this is simple by Clifford's Theorem, so K_i acts irreducibly on V_i. Now $\dim V_i = n_i < n$; hence by induction on n there is a subgroup D_i of K_i such that $|K_i : D_i| \leq g(n_i)$ and D_i acts diagonally on V_i. Define $D = \bigcap_{i=1}^k D_i$; then D is diagonalizable and $|K:D| \leq \prod_{i=1}^k g(n_i) \leq (\max\{g(i) \mid 1 \leq i < n\})^n = l(n)$. Thus $|G:D| \leq (n!)l(n)$. Replace D by its core in G and apply 1.6.9 to obtain the result with $g(n) = ((n!)l(n))!$.

(ii) In the general case form an FG-composition series $0 = V_0 < V_1 < \cdots < V_e = V$. Apply (i) to the group $G/C_G(V_{i+1}/V_i)$, regarded as a subgroup of $\mathrm{GL}(V_{i+1}/V_i)$. If $\dim(V_{i+1}/V_i) = n_i$, we conclude that there is a normal subgroup D_i of index at most $g(n_i)$ which acts diagonally on V_{i+1}/V_i. Then T, the intersection of the D_i, is clearly triangularizable; moreover $|G:T|$ cannot exceed $(\max g(n_i))^n = h(n)$. □

15.1.3 (Zassenhaus). *Let F be any field. Then the derived length of a soluble F-linear group of degree n cannot exceed a number depending only on n. Thus a locally soluble F-linear group is soluble.*

Proof. It suffices to consider a soluble group G of $n \times n$ matrices over an algebraically closed field; for F may be replaced by its algebraic closure. By 15.1.1 there is a normal subgroup T of finite index at most $h(n)$ such that $T \leq T(n, F)$. But T has derived length at most $d = [\log_2(n-1)] + 2$ or 1 if $n = 1$; this was proved in 5.1. Hence the derived length of G is at most $h(n) + d$. The second statement follows from the first. □

The upper bound for the derived length that is furnished by the proof is quite extravagant—for sharp bounds see Newman [a147].

15.1.4 (Mal'cev). *A soluble linear group over a field is a finite extension of a group with nilpotent derived subgroup.*

This is because $T(n, F)/U(n, F)$ is abelian and $U(n, F)$ is nilpotent (see 5.1).

One way of showing that a soluble group is *not* linear is to prove that it does not have the structure prescribed by 15.1.4.

15.1.5. *Let $G = (X \wr Y) \wr Z$ be the standard wreath product of three infinite cyclic groups. Then G is not linear over any field.*

Proof. Suppose that G is linear. Then for some $m > 0$ the subgroup $H = \langle X^m, Y^m, Z^m \rangle$ has nilpotent derived group. But H is simply the standard wreath product of X^m, Y^m and Z^m, so we may as well take $m = 1$.

Let B be the base group of the *outer* wreath product $(X \wr Y) \wr Z$; then $[B, Z]$ is nilpotent, say of class k. Choose a from $X \wr Y$ and write a_i^* for the element of B whose 1-component is a_i and whose other components equal 1. If Z is generated by z, then $[a_i^*, z]$ has its z-component equal to a_i. Hence the z-component of $[[a_1^*, z], \dots, [a_{k+1}^*, z]]$ equals $[a_1, \dots, a_{k+1}]$. It follows that $[a_1, \dots, a_{k+1}] = 1$ and $X \wr Y$ is nilpotent. But this is absurd since $X \wr Y$ has trivial center (Exercise 1.6.14). $\square$

It follows that *a finitely generated soluble group need not be linear* (over any field). On the other hand, L. Auslander has proved that a polycyclic group is always $\mathbb{Z}$-linear (and hence $\mathbb{Q}$-linear): a proof of this (due to R.G. Swan) can be found in [b54] or [b71].

The next theorem provides important information on the structure of polycyclic groups.

15.1.6 (Mal'cev). *A polycyclic group has a normal subgroup of finite index whose derived subgroup is nilpotent.*

Proof. Let G be a polycyclic group. Then there is a normal series $1 = G_0 < G_1 < \cdots < G_e = G$ such that G_{i+1}/G_i is either free abelian of finite rank or finite. Let $K_i = C_G(G_{i+1}/G_i)$. If G_{i+1}/G_i is finite, then so is G/K_i. On the other hand, if G_{i+1}/G_i is infinite, then G/K_i is $\mathbb{Z}$-linear. Extend the action of G/K_i to the complex vector space $(G_{i+1}/G_i) \otimes_{\mathbb{Z}} \mathbb{C}$ and view G/K_i as a $\mathbb{C}$-linear group. By 15.1.1 there is a normal subgroup of finite index in G/K_i which is triangularizable, say T_i/K_i. Then elements of $(T_i/K_i)'$ can be represented by unitriangular matrices. From this it follows that $[G_{i+1}, {}_{m(i)}T_i'] \leq G_i$ for some $m(i) > 0$. We conclude that there is a normal subgroup N of finite index in G such that $[G_{i+1}, {}_m N'] \leq G_i$ for all i and some $m > 0$. This implies that N' is nilpotent. $\square$

EXERCISES 15.1

1. The class of linear groups of given characteristic p is closed with respect to forming subgroups and finite direct products, but not images.

2. The standard wreath product $X \wr Y$ of two infinite cyclic groups is $\mathbb{R}$-linear. [*Hint*: Let $X = \langle x \rangle$, $Y = \langle y \rangle$ and consider the assignments $x \mapsto \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $y \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & \xi \end{smallmatrix}\right)$ where ξ is a real transcendental.]

3. The class of $\mathbb{R}$-linear groups is not extension closed.

4. Let $A \lhd G$ where A is a divisible abelian p-group of rank n. Prove that $\bar{G} = G/C_G(A)$ is linear over the ring of p-adic integers.

5. (R. Strebel). Let G be an F-linear group where F is a field. Prove that $G/\zeta G$ is also F-linear. [*Hint*: Let G act on a vector space V. Regarding G as a subset of $\mathrm{End}_F(V)$, let R be the subring generated by G. Consider the action of G on R via conjugation.]

6. Let G be a group with a series of finite length $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G$ whose factors are abelian. If the sum of the p-ranks of each factor ($p = 0$ or a prime) is finite, then G is said to be a soluble group of *finite total rank*.
   (a) If G is a soluble group with finite total rank, it has a *normal* series of the type specified in the definition.
   (b) (Mal'cev). A soluble group of finite total rank has a subgroup of finite index whose derived subgroup is nilpotent. [*Hint*: Use (a) and imitate the proof of 15.1.6.]

7. (Mal'cev). If A is an abelian subgroup of $\mathrm{GL}(n, \mathbb{Z})$, then A is finitely generated. Proceed as follows.
   (a) Argue by induction on n and show that we may assume A to be rationally irreducible (i.e., irreducible as a subgroup of $\mathrm{GL}(n, \mathbb{Q})$.
   (b) If A acts on the natural rational vector space V, then $\mathrm{End}_{\mathbb{Q}A}(V)$ is division ring by Schur's Lemma, and its center F is an algebraic number field. Argue that A is a group of algebraic units of F. Now apply Dirichlet's theorem on the group of units of a number field (see [b73], for example.)

8. Let A be an irreducible abelian subgroup of $\mathrm{GL}(n, \mathbb{Q})$. If A has finite torsion-free rank, show that it is finitely generated. (For the structure of the multiplicative group of an algebraic number field see [b24].)

15.2. Soluble Groups with Finiteness Conditions on Abelian Subgroups

Intuitively one might expect the abelian subgroups of a soluble group to exert a considerable influence on the structure of the group. For example, it is quite a simple exercise to show that a soluble group is finite if all its abelian subgroups are finite (see Exercise 15.2.1). There are several much deeper theorems of this type, the most famous being due to Mal'cev and Schmidt.

15.2.1 (Mal'cev). *A soluble group G satisfies the maximum condition if each of its abelian subgroups satisfies this condition.*

15.2.2 (Schmidt). *A soluble group G satisfies the minimal condition if each of its abelian subgroups satisfies this condition.*

The reader is reminded that a soluble group with min is a Černikov group (5.4.23) and a soluble group with max is a polycyclic group (5.4.12). Also an abelian group satisfies max precisely when it is finitely generated.

We begin with a simple fact about endomorphisms of torsion-free abelian groups.

15.2.3 (Fuchs). *Let θ be an endomorphism of a torsion-free abelian group A of finite rank. Then θ is injective if and only if $|A : \mathrm{Im}\ \theta|$ is finite.*

Proof. The group A is written additively. If $|A : \mathrm{Im}\ \theta|$ is finite, then A and $\mathrm{Im}\ \theta$ have the same torsion-free rank. Since $A/\mathrm{Ker}\ \theta \simeq \mathrm{Im}\ \theta$, it follows that $\mathrm{Ker}\ \theta = 0$. Conversely let θ be injective. Since A may be thought of as a subgroup of a finite-dimensional rational vector space, we may represent θ by a rational matrix. Thus θ satisfies an equation of the form $l_0 + l_1\theta + \cdots + l_m\theta^m = 0$ where the l_i are integers, not all zero. Here one can assume that $l_0 \neq 0$ because θ is injective. Now $l_0 a = (-l_1 a - l_2 a\theta - \cdots - l_m a\theta^{m-1})\theta \in \mathrm{Im}\ \theta$ for all a in A. This implies that $l_0 A \leq \mathrm{Im}\ \theta$. But $A/l_0 A$ is finite because A has finite rank (Exercise 4.3.9). Hence $|A : \mathrm{Im}\ \theta|$ is finite. □

Two Basic Lemmas

The two lemmas which follow provide the key to the main theorems 15.2.1 and 15.2.2. They should be viewed as weak splitting criteria, giving conditions for a group to split over a normal subgroup "to within finite index" or "up to a finite subgroup."

15.2.4. *Let $A \lhd G$ where A and G/A are abelian and A is torsion-free of finite rank. Assume that every nontrivial G-admissible subgroup of A has torsion quotient group in A. If A is not central in G, then there is a subgroup H such that $|G : HA|$ is finite and $H \cap A = 1$.*

15.2.5. *Let $A \lhd G$ where A and G/A are abelian and A is a divisible group of finite rank. Assume that every proper G-admissible subgroup of A is finite. If A is not central in G, then there is a subgroup H such that $G = HA$ and $H \cap A$ is finite.*

***Proof of* 15.2.4.** Since A is not central, there is an element g of G such that $[A, g] \neq 1$. Hence the mapping $a \mapsto [a, g]$ is a nonzero endomorphism of A, say θ. Since G/A is abelian,

$$[a^x, g] = [a, g^{x^{-1}}]^x = [a, [x^{-1}, g^{-1}]g]^x = [a, g]^x$$

where $a \in A$ and $x \in G$. This shows that θ is a G-endomorphism; hence $\operatorname{Ker} \theta \lhd G$. Now $A/\operatorname{Ker} \theta \simeq \operatorname{Im} \theta \leq A$, so $A/\operatorname{Ker} \theta$ is torsion-free. By the hypothesis on A we have $\operatorname{Ker} \theta = 1$, so that θ is injective. Now apply 15.2.3 to conclude that $|A : \operatorname{Im} \theta|$ is finite, equal to m say. We write $C = C_G(A/\operatorname{Im} \theta)$, observing that $|G : C|$ is finite.

Let $c \in C$; then $[c, g]^m \in \operatorname{Im} \theta$. Now $[c^m, g] \equiv [c, g]^m \operatorname{mod}[C, g, C]$ by one of the elementary commutator formulas. Also $[C, g, C] \leq [A, C] \leq \operatorname{Im} \theta$. Therefore $[c^m, g] \in \operatorname{Im} \theta = [A, g]$ and $[c^m, g] = [a, g]$ for some a in A, from which it follows that $c^m a^{-1} \in C_G(g) = H$, say. Thus $c^m \in HA$ and since $HA \lhd G$, we can conclude that G/HA is an abelian torsion group.

The next step is to show that G/HA is finitely generated; this will force G/HA to be finite. Choose a transversal to $\operatorname{Im} \theta$ in A, say $\{a_1, \ldots, a_m\}$. For $j = 1, 2, \ldots, m$ we select an element x_j in G such that $a_j = [x_j, g]$, with the understanding that $x_j = 1$ should such a choice be impossible. Now pick an element x of G. Since G/A is abelian, $[x, g] = a_i[b_i, g]$ for some i and $b_i \in A$. Thus $[xb_i^{-1}, g] = a_i$, so that $[xb_i^{-1}, g] = [x_i, g]$ and $xb_i^{-1}x_i^{-1} \in C_G(g) = H$. It follows that $x \in \langle x_1, \ldots, x_m, H, A \rangle$, which shows G/HA to be finitely generated.

Finally $H \cap A = \operatorname{Ker} \theta = 1$. □

***Proof of* 15.2.5.** Choose g as in 15.2.4, observing that $a \mapsto [a, g]$ is a G-endomorphism θ of A. Since $\operatorname{Ker} \theta \lhd G$ and $\operatorname{Ker} \theta \neq A$, the hypothesis on A implies that $\operatorname{Ker} \theta$ is finite. Also $1 \neq \operatorname{Im} \theta \lhd G$ and $\operatorname{Im} \theta$ is divisible and therefore infinite. Hence $\operatorname{Im} \theta = A$, again by the hypothesis on A. Thus θ is surjective.

Now choose any element x of G. Then $[x, g] \in A = \operatorname{Im} \theta = [A, g]$, so that $[x, g] = [a, g]$ for some a in A. Hence $xa^{-1} \in C_G(g) = H$, say. We have proved that $x \in HA$, so $G = HA$. Finally $H \cap A = \operatorname{Ker} \theta$ is finite. □

15.2.6. *Let $A \lhd G$ where A is abelian. If every abelian subgroup of G satisfies the maximal condition, then the same is true of abelian subgroups of G/A.*

15.2.7. *Let $A \lhd G$ where A is abelian. If every abelian subgroup of G satisfies the minimal condition, then the same is true of abelian subgroups of G/A.*

***Proof of* 15.2.6.** Suppose that B/A is an abelian subgroup of G/A. We shall prove that B, and hence B/A, is finitely generated.

(i) *Case*: *A is central in B.* Then B is a nilpotent group; let M be a maximal normal abelian subgroup of B. Thus $A \leq M$ and $M = C_B(M)$ by 5.2.3. If $b \in B$, the mapping $xA \mapsto [x, b]$ is a homomorphism from M/A to A—let us call it b^τ. In addition $\tau: B \to \operatorname{Hom}(M/A, A) = L$ is a homomorphism with kernel $C_B(M) = M$. Now L is a finitely generated abelian group since both M/A and A are groups of this type. Therefore B/M is finitely generated, which implies that B is finitely generated.

(ii) *Case*: *A is finite*. Here $C = C_B(A)$ has finite index in B. Also $A \leq \zeta C$, so that C/A is finitely generated by (i). It follows that B is finitely generated.

(iii) *Conclusion*. Let T denote the torsion-subgroup of A; this is finite because A is finitely generated. By (ii) abelian subgroups of G/T are finitely generated, so we may assume that $T = 1$, that is, A is free abelian of finite rank r say.

Let us suppose that the pair (G, A) has been chosen with A of minimal rank subject to the existence of a nonfinitely generated abelian subgroup B/A of G/A. This minimality of rank implies that a nontrivial B-admissible subgroup of A must have finite index in A. Also A is not central in B by (i). Now apply 15.2.4 to conclude that there is a subgroup H with the properties $H \cap A = 1$ and $|B:HA| < \infty$. Then $H \simeq HA/A \leq B/A$, so H is abelian and therefore finitely generated. It follows that HA, and hence B, is finitely generated. □

***Proof of* 15.2.7.** This has the same form as the preceding proof. Let B/A be an abelian subgroup of G/A; it will be enough to prove that B has min.

(i) *Case*: *A is central in B*. Here B is nilpotent; denote by M a maximal normal abelian subgroup of B. As in the preceding proof there is a homomorphism τ from B to $L = \mathrm{Hom}(M/A, A)$ with kernel M. At this point some care must be exercised because L need not satisfy min (why not?). One observes however that τ maps B into the *torsion-subgroup* L_0 of L; in fact L_0 is finite. To see this, pick θ in L_0: then $m\theta = 0$ for some $m > 0$. Writing $\bar{D}$ for the maximal divisible subgroup of $\bar{M} = M/A$, we have $(\bar{D}^\theta)^m = 1$. However $\bar{D}^\theta$ is certainly divisible; thus $\bar{D}^\theta = 1$ and $\bar{D} \leq \mathrm{Ker}\,\theta$. It follows easily that $L_0 \simeq \mathrm{Hom}(\bar{M}/\bar{D}, A)$. Now $\bar{M}/\bar{D}$ is finite in view of the structure of abelian groups with min (4.2.11); let its order be $\bar{m}$. Then a homomorphism from $\bar{M}/\bar{D}$ to A will have its image in A_0, the subgroup of all elements a satisfying $a^{\bar{m}} = 1$. Thus in fact $L_0 \simeq \mathrm{Hom}(\bar{M}/\bar{D}, A_0)$. But A_0 is finite since it has finite exponent and min, so L_0 is finite. In conclusion we see that B/M is finite; thus B has min.

(ii) *Case*: *A is finite*. Argue as in the proof of 15.2.6.

(iii) *Conclusion*. Since A has min, there is a finite characteristic subgroup F such that A/F is divisible. By (ii) we can factor out F; thus assume that A is a divisible p-group.

Suppose that the pair (G, A) has been chosen so that A has minimal rank subject to the existence of an abelian subgroup B/A of G/A that does not have min. By minimality a proper B-admissible subgroup of A is finite. Also A cannot be central in B by (i). We are now in a position to apply 15.2.5. There is a subgroup H such that $B = HA$ and $H \cap A$ is finite. According to (ii) abelian subgroups of $H/H \cap A$ satisfy min. Now $H/H \cap A \simeq HA/A = B/A$, so $H/H \cap A$ is abelian. Consequently B/A has min by (ii); therefore so does B. □

***Proof of* 15.2.1.** Let d denote the derived length of G. If $d \leq 1$, then, G being abelian, there is nothing to prove. Let $d > 1$ and write $A = G^{(d-1)}$. By 15.2.6 abelian subgroups of G/A satisfy max. Hence, by induction on d, the group G/A has max. Therefore G has max. □

***Proof of* 15.2.2.** This proceeds in the same manner via induction on the derived length. □

Minimax Groups

A group is called a *minimax group* if it has a series of finite length whose factors satisfy *either* max *or* min. Thus minimax is a finiteness property which generalizes both max and min. A basic example of an abelian minimax group in the group $\mathbb{Q}_\pi$ of rational numbers whose denominators are π-numbers where π is some finite set of primes: for $\mathbb{Z}$ satisfies max and $\mathbb{Q}_\pi/\mathbb{Z}$ min. It should be clear that an abelian minimax group has finite rank.

Suppose that A is an abelian minimax group; let $1 = A_0 \lhd A_1 \lhd \cdots \lhd A_n = A$ be a series with min or max factors. Choose a finite set of generators for each finitely generated factor of the series; then choose a preimage in A of each generator. The resulting finite set generates a subgroup X such that A/X has min. Thus *an abelian group is minimax if and only if it is an extension of a group with max by a group with min.* However this conclusion does not hold for arbitrary soluble minimax groups (Exercise 15.2.6). Notice that a soluble torsion group is minimax if and only if it has min. (For further properties of abelian minimax groups see Exercise 4.4.7.)

There is a theorem for the property minimax analogous to the theorems of Mal'cev and Schmidt.

15.2.8 (Baer, Zaicev). *A soluble group is minimax if each of its abelian subgroups is minimax.*

In the usual way this follows from

15.2.9. *Let $A \lhd G$ where A is abelian. If every abelian subgroup of G is minimax, then the same is true of abelian subgroups of G/A.*

The standard mode of proof is employed, but the special case where A is central requires extra attention.

***Proof of* 15.2.9.** Clearly we can split the proof into two cases, A torsion and A torsion-free. Let B/A be an abelian subgroup of G/A.

(i) *Case*: *A is central in B.* Suppose that A is a torsion group; let π denote the set of prime divisors of orders of elements of A, a finite set. Consider the torsion-subgroup S/A of B/A. Then S is a torsion group, so its abelian sub-

groups have min. Schmidt's Theorem (15.2.2) implies that S has min. Hence S/A has min and is a direct factor of B/A by 4.3.9. In view of this we can assume that B/A is torsion-free.

Choose any countable subset $\{x_1, x_2, \ldots\}$ of B. If we succeed in proving $X = \langle x_1, x_2, \ldots \rangle$ to be a minimax group, it will follow that B/A has finite rank; also B will be countable and hence a minimax group.

Since B/A is abelian, $[x_i, x_j] \in A$, so that $[x_i, x_j]^{l_{ij}} = 1$ for some positive π-number l_{ij}. Now $[x_i, x_j]$ belongs to the center of B; therefore

$$[x_i, x_j^{l_{ij}}] = 1.$$

Define $l_1 = 1$ and $l_j = l_{1j}l_{2j}\cdots l_{j-1j}$, $(j > 1)$. The above equation shows that the subgroup

$$Y = \langle x_1^{l_1}, x_2^{l_2}, \ldots \rangle$$

is abelian. By hypothesis Y is a minimax group. It follows that YA is a minimax group. Now XA/YA is a π-group, as may be seen from the fact that the l_j are π-numbers. Since YA/A has finite torsion-free rank, so does XA/A; hence XA/YA has finite p-rank for all primes p (see Exercise 4.2.7). Since π is finite, we conclude that XA/YA has min in view of the structure of abelian p-groups with finite p-rank (4.3.13). Hence XA is minimax, which, of course, implies that X is minimax.

Now suppose that A is torsion-free. If M is a maximal normal abelian subgroup of B, then in the usual way we form a homomorphism from B to $L = \mathrm{Hom}(M/A, A)$ with kernel M. Let $\theta \in L$. Since A is torsion-free, the torsion-subgroup T/A of M/A is mapped by θ to 1. Thus θ will be determined by its effect upon a maximal independent subset of M/T. It follows that L is isomorphic with a subgroup of a direct product of finitely many copies of A. This surely implies that L is a minimax group. Hence B is a minimax group.

(ii) *Case*: *A is finite*. The usual argument applies.

(iii) *Conclusion*. By factoring out a finite subgroup of A, we reduce to two special cases: A torsion-free or a divisible p-group. Let (A, G) be chosen so that the rank of A is minimal subject to the existence of an abelian subgroup B/A of G/A that is not minimax. By (i), A is not central in B. The minimality of rank shows that 15.2.4 or 15.2.5 can be applied. Thus there is a subgroup H such that $|B : HA|$ is finite and $H \cap A = 1$ or $B = HA$ and $H \cap A$ is finite. In the usual way H is minimax, whence so is B. □

A complete discussion of soluble groups with finiteness restrictions on their abelian subgroups is to be found in [a171].

Exercises 15.2

1. A soluble group is finite if each of its subnormal abelian subgroups is finite. [*Hint*: Reduce to the case of a metabelian group G. Choose a maximal abelian subgroup A containing G' and observe that $A = C_G(A)$.]

2. A soluble group G satisfies max if each of its subnormal abelian subgroups does. Adopt the following procedure.
   (a) Use induction on the derived length of G to reduce to the case where G has a normal abelian subgroup A and G/A is abelian.
   (b) Reduce to the case where A is free abelian.
   (c) Now apply Exercise 15.1.7.
3. Let $G = \langle t \rangle \ltimes A$ where A is of type 2^∞ and $a^t = a^3$, $(a \in A)$. Prove that every subnormal abelian subgroup of G is contained in A and thus has min, but G does not have min (cf. the previous exercise).
4. Let G be the holomorph of $\mathbb{Q}$. Prove that each subnormal abelian subgroup has torsion-free rank ≤ 1, but G does not have finite torsion-free rank (see Exercise 14.1.1).
5. If G is a nilpotent group such that G_{ab} is minimax, then G is minimax.
6. Give an example of a minimax group that is not an extension of a group with max by a group with min. [*Hint*: The group of Exercise 15.2.3.]
7. (Čarin). If G is a soluble group all of whose abelian subgroups have finite total rank (in the sense of Exercise 15.1.6), then G has finite total rank. [*Hint*: Imitate the proof of 15.2.8.]
8. (Mal'cev). A soluble subgroup of $GL(n, \mathbb{Z})$ is polycyclic. [*Hint*: Apply Exercise 15.1.7.]
9. Give an example of a finitely generated infinite soluble group with all its abelian normal subgroups finite (see Exercise 15.2.1). [*Hint*: Apply 14.1.1 with A a non-trivial finite abelian group.]

15.3. Finitely Generated Soluble Groups and the Maximal Condition on Normal Subgroups

The rest of this chapter is devoted to finitely generated soluble groups. That this is a complex class of groups is indicated by a theorem of Neumann and Neumann ([a145]): *any countable soluble group of derived length d may be embedded in a 2-generator soluble group of derived length at most* $d + 2$. Thus finitely generated soluble groups of derived length 3 can have complicated abelian subgroups. (See also 14.1.1.) This might suggest finitely generated metabelian groups as suitable objects of study. In fact we shall do somewhat better, dealing with finitely generated groups that are extensions of abelian groups by nilpotent (or even polycyclic) groups. Most of the ideas in the theory that follows originated in three fundamental papers of P. Hall published between 1954 and 1961.

We begin by recalling an elementary fact: a soluble group with max-n is finitely generated (5.4.21). Thus for soluble groups the property max-n is intermediate between max and finitely generated. Are there significant

classes of soluble groups which possess max-n other than polycyclic groups? The following theorem, the basic result of the whole theory, furnishes a large class of such groups.

15.3.1 (P. Hall). *A finitely generated group G which is an extension of an abelian group by a polycyclic group satisfies the maximal condition on normal subgroups.*

For example, a finitely generated metabelian group has max-n. So the standard wreath product of a pair of infinite cyclic groups has max-n, but it is not polycyclic since it does not satisfy max.

The main ingredient in the proof of 15.3.1 is a variant of Hilbert's Basis Theorem on polynomial rings. This is the first of a series of well-known results from commutative algebra that underlie the principal theorems of this and the following sections. (The reader who wishes to read about the background should consult a text on commutative algebra; however this is not necessary to comprehend the sequel.)

The version of Hilbert's Basis Theorem referred to now follows.

15.3.2 (P. Hall). *Let G be a group with a normal subgroup H and let R be a ring with identity. Assume that G/H is either infinite cyclic or finite. Suppose that M is an RG-module and N an RH-submodule. If N generates M as an RG-module and N is RH-noetherian, then M is RG-noetherian.*

Recall that a (right) module over a ring S is said to be *noetherian*, or to satisfy max-S in the notation of 3.1, if it satisfies the maximal condition on S-submodules. A ring S is said to be *right noetherian* if S_S, the ring S regarded as a right S-module in the obvious way, is noetherian: this amounts to imposing the maximal condition on the right ideals of S.

If we take H to be 1, $G = \langle t \rangle$ an infinite cyclic group and R a right noetherian ring, the theorem shows that $R\langle t \rangle$ is right noetherian. Since $R\langle t \rangle$ is the polynomial ring $R[t, t^{-1}]$, the connection with the polynomial ring form of Hilbert's theorem becomes apparent.

Proof of **15.3.2.** (i) Suppose first of all that G/H is finite. Let $\{t_1, \dots, t_l\}$ be a transversal to H in G. Since $G = \bigcup_{i=1} Ht_i$ and by hypothesis $M = (N)RG$, we have $M = Nt_1 + \cdots + Nt_l$. Now if $a \in N$ and $x \in H$, then $(at_i)x = (ax^{t_i^{-1}})t_i \in Nt_i$, which implies that Nt_i is an RH-submodule. The same equation makes it clear that the mapping $a \mapsto at_i$ is an R-isomorphism which maps RH-submodules of N to RH-submodules of Nt_i. (However it is not an RH-isomorphism) Since N has max-RH, so must Nt_i. Therefore M satisfies max-RH, by 3.1.7. *A fortiori* M satisfies max-RG.

(ii) Now let G/H be infinite cyclic, generated by Ht let us say. Then each element a of M can be written in the form

$$a = \sum_{i=r}^{s} b_i t^i$$

where $b_i \in N$ and $r \leq s$, although perhaps not in a unique fashion. If $b_s \neq 0$, call $b_s t^s$ a *leading term* and b_s a *leading coefficient* of a.

Choose a nonzero RG-submodule M_0 of M. Our task is to show that M_0 is finitely generated as an RG-module; for by 3.1.6 this will imply that M is RG-noetherian. To this end we form the set N_0 consisting of 0 and all leading coefficients of elements of M_0, claiming that N_0 is a RH-submodule of N. To see this suppose that a and a' belong to M_0, having leading terms $b_s t^s$ and $b'_{s'} t^{s'}$. Then $a \pm a' t^{s-s'}$ certainly belongs to M_0; moreover its leading coefficient is $b_s \pm b'_{s'}$ unless of course this vanishes. Thus in any event $b_s \pm b'_{s'} \in N_0$. Furthermore, if $u \in RH$, then $a(t^{-s}ut^s)$ in M_0 has leading term $(b_s u)t^s$ unless $b_s u = 0$; hence $b_s u \in N_0$ and our claim is established.

By hypothesis N has max-RH. Hence there is a finite set $\{b, \dots, b_l\}$ with $b_i \neq 0$ which generates N_0 as an RH-module. By definition there exists an a_i in M_0 which has b_i as a leading coefficient. Now we can modify a_i by a large enough power of t to ensure that no negative powers of t are involved: the same device permits us to assume that $b_i t^m$ is a leading term of a_i for each i. Thus all the a_i have leading terms of the same degree n.

Next define M_1 to be the RG-submodule generated by $a_1, \dots, a_l$. Also write $N_1 = M_0 \cap (N + Nt + \cdots + Nt^{m-1})$. Observe that $N + Nt + \cdots + Nt^{m-1}$ has max-RH by an argument used in the first paragraph; consequently its RH-submodule N_1 is finitely generated. Therefore the RG-module

$$M_2 = M_1 + (N_1)RG$$

is finitely generated. Now obviously $M_2 \leq M_0$; our contention is that $M_2 = M_0$, which will complete the proof.

Suppose that $a \in M_0 \backslash M_2$. Certainly there is nothing to be lost in assuming that a does not involve negative powers of t. Choose such an element a whose leading term is ct^p where p is as small as possible. If $p < m$, then $a \in M_0 \cap (N + Nt + \cdots + Nt^{m-1}) = M_1 \leq M_2$, which is not true; thus $p \geq m$. Since $c \in N_0$, it is possible to write $c = \sum_{i=1}^{l} b_i u_i$ where $u_i \in RH$. Now the element

$$a' = \sum_{i=1}^{l} a_i(t^{-m}u_i t^p)$$

belongs to M_2, involves no negative powers of t and has a leading term

$$\left(\sum_{i=1}^{l} b_i u_i\right) t^p = ct^p.$$

So a and a' have the same leading term. Hence $a - a'$ belongs to $M_0 \backslash M_2$ and involves no powers of t higher than the $(p-1)$th, which contradicts the minimality of p. □

The important application of this lemma is to the group ring of a polycyclic group.

15.3.3 (P. Hall). *Let G be a finite extension of a polycyclic group and let R be a right noetherian ring with identity. Then the group ring RG is right noetherian.*

Proof. By hypothesis there is a series $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ whose factors are infinite cyclic or finite. If $n = 0$, then $G = 1$ and $RG = R$, which is given as being right noetherian. Let $n > 0$ and put $H = G_{n-1}$. By induction on n the ring RH is right noetherian, that is, as an RH-module it has max-RH. Apply 15.3.2 with $M = RG$ and $N = RH$ to get the result. □

On the basis of 15.3.3 it is now easy to complete the proof of 15.3.1.

***Proof of* 15.3.1.** By hypothesis G possesses a normal abelian subgroup A such that $H = G/A$ is polycyclic. View A as a $\mathbb{Z}H$-module by conjugation in the natural way. Now G is finitely generated, while H is finitely presented since it is polycyclic (see 2.2.4); hence A is a finitely generated $\mathbb{Z}H$-module by 14.1.3. Consequently, in additive notation, A is a sum of finitely many cyclic $\mathbb{Z}H$-modules. But a cyclic $\mathbb{Z}H$-module has max-$\mathbb{Z}H$ since it is an image of $\mathbb{Z}H$ and the latter is right noetherian as a ring by 15.3.3. It follows that A has a max-$\mathbb{Z}H$ or, what is the same thing, max-G. Finally G has max-G, that is to say max-n. □

Not every finitely generated soluble group has max-n: for example, the group G of 14.1.1 does not have max-n if A is not finitely generated. Notice that this group has derived length 3, confirming the bad behaviour of finitely generated soluble groups with derived length greater than 2.

The Upper and Lower Central Series in Finitely Generated Abelian-by-Nilpotent Groups

The next objective is to prove some results about the lengths of the upper and lower central series in finitely generated soluble groups. In the background here is a key theorem of commutative algebra known as the *Artin–Rees property* (see Exercise 15.3.4). The small amount of ring theory necessary will be developed from scratch.

Polycentral Ideals

Let R be a ring with identity element. Recall that an element r is said to be *central* in R if $rx = xr$ for all x in R. The set of all central elements is a subring of R, the *center*. An ideal I is called a *central ideal* of R if it can be generated by central elements; thus $I = \sum_\lambda r_\lambda R = \sum_\lambda Rr_\lambda$ where each r_λ is central. It is important to notice that $JI = IJ$ if J is any ideal and I any central ideal of R.

More generally an ideal I is said to be *polycentral* if there is a finite series of ideals of R

$$0 = I_0 < I_1 < \cdots < I_l = I$$

which is *R-central*, that is to say, I_{i+1}/I_i is a central ideal of R/I_i. The length of a shortest series of this type is the *height* of I.

To explain the relevance of polycentral ideals let us consider a group G and a normal subgroup H which is contained in some finite term of the upper central series, say $H \leq \zeta_c(G)$. Defining $H_i = H \cap \zeta_i G$, we obtain a series $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_c = H$ which is a partial central series of G. Let $I_i = \bar{I}_{H_i}$ be the right ideal of $\mathbb{Z}G$ generated by all elements $x - 1$ where $x \in H_i$; it was shown in 11.3 that I_i is a two sided ideal of $\mathbb{Z}G$. Also of course $O = I_0 \leq I_1 \leq \cdots \leq I_c = \bar{I}_H$. In fact this is a central series in $\mathbb{Z}G$, so that $\bar{I}_H$ is a polycentral ideal of $\mathbb{Z}G$. To prove this choose $x \in H_{i+1}$ and $g \in G$; then

$$(x - 1)g - g(x - 1) = xg - gx = gx([x, g] - 1).$$

Since $[x, g] \in H_i$, it follows that $[x, g] - 1 \in I_i$ and $(x - 1)g \equiv g(x - 1) \bmod I_i$. Therefore I_{i+1}/I_i is a central ideal of $\mathbb{Z}G/I_i$.

In particular $\bar{I}_H$ is polycentral in $\mathbb{Z}G$ whenever $H \lhd G$ and G is nilpotent. This will be our standard example of a polycentral ideal.

We proceed now to establish the necessary facts about polycentral ideals.

15.3.4. *Let R be a ring with identity and let M be a right noetherian R-module. Suppose that J is a sum of polycentral ideals of R each of which has a power annihilating M. Then $MJ^n = 0$ for some $n > 0$.*

Proof. Since M is noetherian, $MJ = MI$ where $I = I(1) + \cdots + I(r)$; here each $I(j)$ is a polycentral ideal of R and $MI(j)^m = 0$ for some $m > 0$. Let $n_1 = r(m - 1) + 1$. Then I^{n_1} is the sum of all products of n_1 $I(j)$'s and in each product at least one $I(j)$ will occur m times; therefore $MI^{n_1} = 0$.

It is clear from the definition that I is polycentral; let

$$0 = I_0 < I_1 < \cdots < I_s = I$$

be a central series of ideals of R. If $MI = 0$, then $MJ = 0$ and there is nothing more to prove. Assume therefore that $MI \neq 0$; then there is an integer $i < s$ such that $0 = MI_i < MI_{i+1}$. The polycentral ideal I/I_{i+1} has height $s - i - 1 < s$ in R/I_{i+1}; by induction hypothesis on the height applied to the R/I_{i+1}-module M/MI_{i+1} there is an $n_2 > 0$ such that $MJ^{n_2} < MI_{i+1}$. Since I_{i+1}/I_i is a central ideal, $I_{i+1}J \leq JI_{i+1} + I_i$. But $MI_i = 0$, so in fact $NI_{i+1}J \leq NJI_{i+1}$ for every submodule N of M. Applying this inclusion repeatedly we deduce that $MJ^{kn_2} \leq MI_{i+1}^k$ for all $k > 0$. Setting $k = n_1$ and remembering that $MI^{n_1} = 0$, we conclude that $MJ^{n_1 n_2} = 0$. □

The crucial property of polycentral ideals can now be established. If M is a right R-module and X a subset of R, let

$$*X$$

denote the set of all a in M which are annihilated by X; thus

$$*X = \{a \in M \mid aX = 0\}.$$

15.3.5 (Robinson). *Let R be a ring with identity and let M be a (right) noetherian R-module. Then there is a positive integer n such that $MI^n \cap *I = 0$ for every polycentral ideal I of R.*

Proof. (i) First we will prove the weaker statement wherein the "n" is allowed to depend on the ideal. Suppose that this has been proved for all ideals of height less than i (where $i > 0$). Choose a polycentral ideal I of height i. Assuming the result false for I, we may suppose the pair (M, I) to be chosen so that the result is true for $(\bar{M}, I)$ whenever $\bar{M}$ is a proper image of M: here we make use of the noetherian condition. Suppose that there are nontrivial submodules M_1 and M_2 such that $M_1 \cap M_2 = 0$. Then by choice of (M, I) there is an integer $n > 0$ such that $MI^n \cap *I \leq M_1$ and $MI^n \cap *I \leq M_2$. This implies that $MI^n \cap *I = 0$, a contradiction. Consequently nontrivial submodules of M intersect nontrivially.

By hypothesis there is a central series of ideals $0 = I_0 < I_1 < \cdots < I_i = I$. Choose a central element x lying in I_1. Then $0 \neq *I \leq *x$, so that $*x \neq 0$. Because x is central in R, the mapping $a \mapsto ax^n$ is an R-endomorphism of M; thus its kernel $*(x^n)$ is a submodule. Since $*x \leq *(x^2) \leq \cdots$, the noetherian condition tells us that there is an integer n_1 such that $*(x^{n_1}) = *(x^{n_1+1})$. Suppose that $a \in Mx^{n_1} \cap *x$; then $a = bx^{n_1}$ for some $b \in M$, and $0 = ax = bx^{n_1+1}$, so that $b \in *(x^{n_1+1}) = *(x^{n_1})$ and $a = bx^{n_1} = 0$. It follows that $Mx^{n_1} \cap *x = 0$. Since Mx^{n_1} and $*x$ are submodules and $*x \neq 0$, we deduce that $Mx^{n_1} = 0$. Now because x is central, $(Rx)^{n_1} = Rx^{n_1}$, so that $M(Rx)^{n_1} = 0$. But I_1 is a sum of ideals of the form Rx with x central. Hence $MI_1^{n_2} = 0$ for some $n_2 > 0$ by 15.3.4.

Suppose we have shown that $MI^rI_1^{s+1} = 0$ for some integers r and s. Then $MI^rI_1^s$ is an R/I_1-module; also I/I_1 is a polycentral ideal of R/I_1 with height $i - 1$. Induction on i yields an integer t such that

$$0 = (MI^rI_1^s)I^t \cap *I = MI^{r+t}I_1^s \cap *I$$

since $I_1 I = I(I_1)$ by centrality of I_1. Because $*I \neq 0$, it follows that $MI^{r+t}I_1^s = 0$. But we know that $MI_1^{n_2} = 0$; thus repeated applications of the foregoing argument lead to $MI^n = 0$ for some $n > 0$. This is a contradiction.

(ii) It remains to show that an "n" can be found which is independent of I. Assume that no such integer exists for M, but that every proper image of M has one. Just as above nontrivial submodules of M must intersect nontrivially. If I is any polycentral ideal, we have proved that there is an integer n_1, depending on I, such that $MI^{n_1} \cap *I = 0$. It follows that either $MI^{n_1} = 0$ or $*I = 0$. Denote by J the sum of all the polycentral ideals of R which have a power annihilating M. Then by 15.3.4 there is an $n > 0$ such that $MJ^n = 0$. Consequently $MI^n \cap *I = 0$ holds for *any* polycentral ideal I. □

Applications

15.3.6 (Stroud, Lennox–Roseblade). *Let G be a finitely generated group with a normal abelian subgroup A such that G/A is nilpotent. Then there is a positive integer n such that*

$$\gamma_n H \cap \zeta H = 1$$

and

$$\zeta_{n-1} H = \zeta_n H$$

for every subgroup H such that $HA \lhd G$.

Proof. Let $R = \mathbb{Z}(G/A)$ and define I to be $\bar{I}_{HA/A}$; this is polycentral in R because $HA/A \lhd G/A$ and G/A is nilpotent. Also G/A is polycyclic, so A is a noetherian R-module by 15.3.1. Thus 15.3.5 is applicable: there is an integer n_1 such that $AI^{n_1} \cap {}^*I = 0$. Now, allowing for the change from additive to multiplicative notation, we recognize AI as $[A, H]$; so in group-theoretic terms $[A, {}_{n_1}H] \cap C_A(H) = 1$. If G/A has nilpotent class c, then $\gamma_{c+1} H \leq A$ and thus $\gamma_{c+1+n_1} H \cap \zeta H = 1$.

The second part is now easy. Writing n for $c + 1 + n_1$, we have $[\zeta_n H, {}_{n-1}H] \leq \gamma_n H \cap \zeta H = 1$, which shows that $\zeta_n H = \zeta_{n-1} H$. □

15.3.7 (Stroud). *Let G be as in* 15.3.6 *and let $H \lhd G$. Then $\gamma_\omega H = \gamma_{\omega+1} H$.*

Proof. Clearly $\gamma_{\omega+1} H \lhd G$, while

$$\gamma_\omega H / \gamma_{\omega+1} H = \gamma_\omega (H/\gamma_{\omega+1} H) \leq \zeta(H/\gamma_{\omega+1} H).$$

Hence $\gamma_\omega H = \gamma_{\omega+1} H$ by 15.3.6. □

For example, if G is a finitely generated metabelian group, there is a finite upper bound for the length of the upper central series of an arbitrary subgroup; for in 15.3.6 we can take A to be G', in which event $HA \lhd G$ is automatic. Also the lower central series of a normal subgroup of G terminates after at most ω steps.

A very extensive theory of upper central lengths of subgroups in finitely generated soluble groups has been developed by Lennox and Roseblade [a123].

Powers of the Augmentation Ideal

15.3.8. *Let R be a ring with identity element, I a polycentral ideal and M a right noetherian R-module. Then an element a belongs to MI^n for every $n > 0$ if and only if $a = ax$ for some x in I.*

Proof. Suppose that $a \in MI^n$ for all n, and consider $N = aI$ and the R-module M/N. According to 15.3.5 there is a positive integer n such that

$(M/N)I^n \cap {}^*I = 0$. Clearly $a + N$ belongs to every $(M/N)I^n$: it also belongs to $^*I$ since $N = aI$. Therefore $a \in N$, which implies that $a = ax$ for some x in I. The converse is obvious. □

The reader may recognize 15.3.8 as a generalization of the *Krull Intersection Theorem* for modules over a commutative ring.

From 15.3.8 we easily obtain a criterion for residual nilpotence of finitely generated soluble groups.

15.3.9. *Let G be a finitely generated group with a normal abelian subgroup A such that G/A is nilpotent. Assume that A is torsion-free as a $\mathbb{Z}(G/A)$-module. Then G is residually nilpotent.*

Proof. Suppose that $1 \neq a \in [A, {}_nG]$ for every n. Apply 15.3.8 with $M = A$, $R = \mathbb{Z}(G/A)$ and $I = I_{G/A}$, the augmentation ideal. Then, in additive notation, $0 \neq a = ax$ for some x in I, or $a(x - 1) = 0$. Since A is a torsion-free R-module, $x = 1$. But $1 \in I$ implies that $I = R$, a contradiction. It follows that the intersection of all the $[A, {}_nG]$ is 1. Since the quotient group $G/[A, {}_nG]$ is nilpotent, G is residually nilpotent. □

In order to make use of this criterion it is necessary to discover situations where the module condition is satisfied. This is the purpose of the ensuing discussion.

Zero Divisors in Group Rings

There is a long-standing conjecture that the integral group ring of a torsion-free group G contains no divisors of zero; equivalently, is $\mathbb{Z}G$ when regarded as a right $\mathbb{Z}G$-module torsion-free? The conjecture has been proved in various special cases, the following one being quite sufficient for our purposes.

15.3.10 (G. Higman). *If G is a group such that every nontrivial finitely generated subgroup has an infinite cyclic image, then $\mathbb{Z}G$ has no zero divisors.*

Proof. Suppose that $ab = 0$ where a and b are nonzero elements of $\mathbb{Z}G$. Let the number of group elements involved in a and in b be m and n respectively. If $l = m + n$, then certainly $l \geq 2$, while $l = 2$ means that $a \in G$ and $b \in G$, which clearly excludes $ab = 0$. Thus $l > 2$. Assume that a and b have been chosen so that l is minimal subject to $ab = 0$. Observe that 1 can be assumed to occur in both a and b; for we can premultiply a and postmultiply b by suitable elements of G to achieve this.

The totality of elements involved in a and b generates a nontrivial finitely generated subgroup H which, by hypothesis, has a normal subgroup K such

that H/K is infinite cyclic, generated by Kt say. We can write

$$a = a_1 t^{u_1} + \cdots + a_r t^{u_r} \qquad \text{and} \qquad b = b_1 t^{v_1} + \cdots + b_s t^{v_s}$$

where $a_i, b_j \in \mathbb{Z}K$ and the integers u_i, v_j satisfy $u_1 < u_2 < \cdots < u_r$ and $v_1 < v_2 < \cdots < v_s$. Suppose that $r = 1 = s$. Since 1 occurs in a and b, and H/K is infinite cyclic, it follows that a and b lie in $\mathbb{Z}K$; however this implies that $H = K$. Hence either $r > 1$ or $s > 1$.

Now form the product ab using the sums exhibited above. The lowest power of t which occurs in the product is $t^{u_1+v_1}$ and its coefficient $a_1 b_1^{t^{-u_1}}$ must therefore be 0. However, because $r > 1$ or $s > 1$, either a_1 involves fewer group elements than a or $b_1^{t^{-u_1}}$ involves fewer than b. This contradicts the minimality of l. □

Obviously a nontrivial poly-infinite cyclic group has an infinite cyclic image. Therefore we obtain the following result.

15.3.11. *The integral group ring of a group that is locally poly-infinite cyclic contains no divisors of zero. In particular this is true of the integral group ring of a finitely generated torsion-free nilpotent group.*

For an account of the present status of the zero divisor problem the reader should consult [b51].

We can now give some examples of groups to which the residual nilpotence criterion applies.

15.3.12. *If $R \rightarrowtail F \twoheadrightarrow G$ is a finite presentation of a finitely generated torsion-free nilpotent group G, then F/R' is residually nilpotent.*

Proof. R_{ab} is a G-module via conjugation in F. It was shown in 11.4.8 that the mapping $rR' \mapsto (r - 1) + I_F \bar{I}_R$ is a $\mathbb{Z}G$-monomorphism from R_{ab} to $I_F/I_F\bar{I}_R$; furthermore the latter module is $\mathbb{Z}G$-free (11.3.4). Now $\mathbb{Z}G$ has no zero divisors by 15.3.11; hence a free $\mathbb{Z}G$-module, and so a submodule of a free $\mathbb{Z}G$-module, is torsion-free. Conclude that R_{ab} is torsion-free as a $\mathbb{Z}G$-module. 15.3.9 can now be applied to give the result. □

For example, let F be a finitely generated free group. It is known that the lower central factors of F are free abelian groups (see for example [b31]). Hence $F/\gamma_n F$ is torsion-free. Thus *the relatively free group $F/(\gamma_n F)'$ is residually nilpotent*, as one sees by taking R to be $\gamma_n F$ in 15.3.12.

The section closes with an interesting application of the intersection theorem 15.3.8.

15.3.13 (Gruenberg). *If G is a finitely generated torsion-free nilpotent group, then the intersection of all the powers of the augmentation ideal I_G is zero.*

Proof. $\mathbb{Z}G$ is torsion-free as a $\mathbb{Z}G$-module by 15.3.11. The result now follows from 15.3.8 with $R = \mathbb{Z}G$ and $I = I_G$. □

In fact 15.3.13 is more generally true: G can be an arbitrary torsion-free nilpotent group (Hartley [a82]).

EXERCISES 15.3

1. If the integral group ring of G is right noetherian, then G satisfies max. [*Hint*: If $H < K \leq G$, then $\bar{I}_H < \bar{I}_K$.]
2. Let $W = \mathbb{Z} \wr G$, the standard wreath product.
   (a) If W satisfies max-*n*, show that G satisfies max.
   (b) If G is a finite extension of a polycyclic subgroup, prove that $\mathbb{Z} \wr G$ satisfies max-*n*. (*Note*: The base group of W is isomorphic with $\mathbb{Z}G$).
3. Let G be a finitely generated extension of an abelian group by a nilpotent group. Prove that the Hirsch–Plotkin radical of G is nilpotent and equals the Fitting subgroup. [*Hint*: Use 15.3.6. See also 15.5.1.]
4. Let R be a ring with identity, I an ideal of R and M a right R-module. The pair (M, I) has the *Artin–Rees property* if, given a submodule N and a positive integer n, there exists a positive integer m such that $MI^m \cap N \subseteq NI^n$. If M is noetherian and I is polycentral in R, prove that (M, I) has the Artin–Rees property.
5. If the integral group ring of G has no zero divisors, then G is torsion-free.
6. If G is a finitely generated torsion-free nilpotent group, the standard wreath product $\mathbb{Z} \wr G$ is residually nilpotent.
7. (P. Hall). There are only countably many nonisomorphic finitely generated groups which are extensions of abelian groups by polycyclic groups. (cf. 14.1.1). [*Hint*: Use 15.3.1.]
8. Let R be a noetherian integral domain and let I be a proper ideal. Prove that $\bigcap_{n=1,2,\ldots} I^n = 0$.

15.4. Finitely Generated Soluble Groups and Residual Finiteness

The principal aim of this section is to prove the following major result.

15.4.1 (P. Hall). *A finitely generated group which is an extension of an abelian group by a nilpotent group is residually finite.*

Like so many results in the theory of finitely generated soluble groups 15.4.1 hinges on properties of finitely generated modules over noetherian group rings. In this instance we require an analogue of what in commutative algebra is known as the *Weak Nullstellensatz* of Hilbert.

The Class of Modules $\mathscr{M}(J, \pi)$

Suppose that J is a principal ideal domain and let π be a set of (non-associate) primes in J. Then a J-module M is said to be belong to the class $\mathscr{M}(J, \pi)$ if it has a free J-submodule F such that M/F is a π-torsion-module; thus if $a \in M$, there is some product x of primes in π such that $ax \in F$. The crucial property of a module in $\mathscr{M}(J, \pi)$ is that it cannot have a submodule isomorphic with the field of fractions of J unless π is a complete set of primes. We list this with other simple facts about $\mathscr{M}(J, \pi)$ in the following lemma.

15.4.2. (i) *If $M \in \mathscr{M}(J, \pi)$ and N is a submodule of M, then $N \in \mathscr{M}(J, \pi)$.*

(ii) *The field of fractions of J belongs to $\mathscr{M}(J, \pi)$ if and only if π is a complete set of primes.*

(iii) *If M has an ascending series of submodules each factor of which belongs to $\mathscr{M}(J, \pi)$, then $M \in \mathscr{M}(J, \pi)$.*

Proof. (i) Since J is a principal ideal domain, a submodule of a free J-module is free. The result now follows easily.

(ii) This is a simple exercise which we leave to the reader.

(iii) Let $0 = M_0 \leq M_1 \leq \cdots M_\alpha = M$ be the given ascending series. By hypothesis there is for each $\beta < \alpha$ a free J-module $\overline{M}_\beta/M_\beta$ such that $M_{\beta+1}/\overline{M}_\beta$ is a π-torsion module. Choose a basis $\{a_{\beta\lambda} + M_\beta | \lambda \in \Lambda(\beta)\}$ for the free module $\overline{M}_\beta/M_\beta$; then form the submodule S generated by all the $a_{\beta\lambda}$ where $\lambda \in \Lambda(\beta)$, $\beta < \alpha$. If there were a nontrivial J-linear relation in the $a_{\beta\lambda}$'s, there would be such a relation in the $a_{\beta\lambda} + M_\beta$ for some fixed β, which is impossible. Consequently the $a_{\beta\lambda}$ are linearly independent over J and S is a free J-module. On the other hand, each $(M_{\beta+1} + S)/(M_\beta + S)$ is a π-torsion module, which clearly implies that M/S is a π-torsion module. □

Now for the basic result on modules over polycyclic group rings which will eventually lead to a proof of 15.4.1.

15.4.3. *Let G be a polycyclic group and J a principal ideal domain. Then a finitely generated JG-module M belongs to the class $\mathscr{M}(J, \pi)$ where π is some finite set of primes in J.*

Proof. Form a series in G with cyclic factors, $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_l = G$. If $l = 0$, then $G = 1$ and M is a finitely generated J-module. The structure theorem for finitely generated modules over principal ideal domains implies the result immediately. So we assume that $l > 0$ and put $N = G_{l-1}$. In what follows we shall write R for JG and S for JN.

(i) *Case*: *G/N is finite.* Choose a transversal T to N in G. Now by hypothesis there is a finite set $\{a_1, a_2, \ldots, a_k\}$ such that $M = a_1R + a_2R + \cdots + a_kR$; hence M is the sum of the finite set of cyclic S-modules $(a_i t)S$, $i = 1$,

$2, \dots, k, t \in T$. Thus M is a finitely generated S-module. By induction on l we obtain $M \in \mathscr{M}(J, \pi)$ for some finite set of primes π.

(ii) *Case*: *G/N is infinite.* Write $G = \langle t, N\rangle$ and $H = \langle t\rangle$. Then $G = H \ltimes N$, the natural semidirect product. Since M is finitely generated as an R-module, there is a finitely generated S-module L such that $M = LR$; hence M is the sum of the S-submodules Lt^i, $i = 0, \pm 1, \pm 2, \dots$.

Now define for each positive integer n

$$L_n^+ = \sum_{i=1}^{n} Lt^i \qquad \text{and} \qquad L_n^- = \sum_{i=-n}^{-1} Lt^i.$$

These are, of course, S-modules, as is $V = \bigcup_{n=1,2,\dots} L_n^-$, the sum of all the Lt^i for negative i. Clearly $V \leq Vt \leq Vt^2 \leq \cdots$, the union of this chain being M. The S-modules Vt/V and Vt^{n+1}/Vt^n are J-isomorphic via the obvious mapping $at + V \mapsto at^{n+1} + Vt^n$. Now $Vt = V + L$, so $Vt/V \simeq^S L/V \cap L$. But $L/V \cap L \in \mathscr{M}(J, \pi_1)$ for some finite π_1 by induction on l. Consequently $M/V \in \mathscr{M}(J, \pi_1)$ by 15.4.2(iii). Thus it remains only to deal with V.

Certainly $0 = L_0^- \leq L_1^- \leq \cdots$ and V is the union of this chain. Also $L_{n+1}^- = Lt^{-(n+1)} + L_n^-$, so that L_{n+1}^-/L_n^- is S-isomorphic with

$$Lt^{-(n+1)}/Lt^{-(n+1)} \cap L_n^-,$$

which is J-isomorphic to $L/L \cap L_n^- t^{n+1} = L/L \cap L_n^+$. Now $L \cap L_1^+ \leq L \cap L_2^+ \leq \cdots$ is an ascending chain of S-submodules of L. Moreover S is right noetherian by 15.3.3—notice here that J is noetherian since it is a principal ideal domain. Since L is a finitely generated S-module, it is noetherian. It follows that $L \cap L_n^+ = L \cap L_{n+1}^+ =$ etc. for some integer n. We see now with the aid of the induction hypothesis that every L_{n+1}^-/L_n^- belongs to $\mathscr{M}(J, \pi_2)$ for some finite set of prime π_2. Therefore $V \in \mathscr{M}(J, \pi_2)$ and $M \in \mathscr{M}(J, \pi)$ where $\pi = \pi_1 \cup \pi_2$. □

On the basis of this lemma the analogue of the *Weak Nullstellensatz* referred to above can be derived.

15.4.4 (P. Hall). *If G is a finitely generated nilpotent group, then any simple $\mathbb{Z}G$-module M is finite.*

Proof. There is nothing to be lost in assuming that G acts faithfully on M; thus we may regard G as a group of automorphisms of M. Because M is simple, it is a cyclic $\mathbb{Z}G$-module; it follows via 15.4.3 that $M \in \mathscr{M}(\mathbb{Z}, \pi)$ for some finite set of primes π. Now the additive group of M is either an elementary abelian p-group or a rational vector space (since it is characteristically simple). However the latter is impossible because $\mathbb{Q}$ cannot belong to $\mathscr{M}(\mathbb{Z}, \pi)$ if π is finite (by 15.4.2). Hence M is an elementary abelian p-group.

Choose z from the center of G. Define J to be the group algebra of an infinite cyclic group $\langle t\rangle$ over F, the field of p elements: thus J is a principal

ideal domain. We make M into a JG-module by defining at to be az for $a \in M$. (Here it is relevant that $z \in \zeta(G)$.) Then $M \in \mathscr{M}(J, \pi)$ for some finite set of primes π of J. Since a complete set of primes for J is infinite, the field of fractions K of J does not occur as a submodule of M: here use is made of 15.4.2 once again.

Since M is a simple JG-module, Schur's Lemma (8.1.4) tells us that $\text{End}_{JG}(M)$ is a division ring; its center C is therefore a field, clearly of characteristic p. By identifying y in F with $y1$ in C, we can regard F as a subfield of C. Let S denote the subring of C generated by F and z. Then the assignment $t \mapsto z$ determines a surjective ring homomorphism α from $J = F\langle t \rangle$ to S. Thus $S \simeq J/I$ for some ideal I.

Suppose that $I = 0$, so that $\alpha: J \to C$ is a monomorphism; this extends to a monomorphism $\alpha: K \to C$. Let $0 \neq a \in M$ and define $\theta: K \to M$ by $x\theta = ax^{\alpha}$, $x \in K$. This is easily seen to be a J-monomorphism. However this cannot be correct since K is not isomorphic with a J-submodule of M. Hence $I \neq 0$.

It now follows that J/I is finite since I is a principal ideal; thus S is finite and z has finite order.

We have now proved that the center of the finitely generated nilpotent group G is a torsion group. It follows via 5.2.22 that G is finite. Since $M = \langle ag \mid g \in G \rangle$ for any nonzero a in M, we conclude that M is finite. □

The main theorem 15.4.1 can now be proved.

***Proof of* 15.4.1.** By hypothesis G is a finitely generated group with a normal abelian subgroup A such tht G/A is nilpotent. Let $1 \neq g \in G$. By Zorn's Lemma there is a normal subgroup which is maximal subject to not containing g—let us call it N. It suffices to prove that G/N is finite. Clearly we lose nothing in supposing N to be trivial. Every nontrivial normal subgroup of G must now contain g. Hence there is a unique smallest nontrivial normal subgroup of G, say M.

If $A = 1$, then G is nilpotent and M lies in the center of G; what is more, M must have prime order, say p. Since M lies in every nontrivial normal subgroup, ζG is a p-group. It follows that G is finite.

Assume that $A \neq 1$, so that $M \leq A$. Now M is a simple $\mathbb{Z}(G/A)$-module, so 15.4.4 shows M to be finite. Thus $C = C_G(M)$ has finite index in G. Now by 15.3.6 there is a positive integer n such that $\gamma_n(C) \cap \zeta C = 1$. But it is clear that $M \leq \zeta C$, so $\gamma_n(C) \cap M = 1$, which can only mean that $\gamma_n C = 1$ and C is nilpotent. Also C is finitely generated since $|G : C|$ is finite. Thus ζC is a finitely generated abelian group; hence some power $(\zeta C)^m$ is torsion-free. But $(\zeta C)^m \cap M = 1$ because M is finite. Consequently $(\zeta C)^m = 1$, which implies that C, and hence G, is finite. □

More recently it has been shown that 15.4.1 is true for the more general class of finitely generated extensions of abelian groups by polycyclic groups. This is due to Jategaonkar [a107] and Roseblade [a180]: the proof is significantly harder.

EXERCISES 15.4

1. Let J be a principal ideal domain and F its field of fractions. Prove that $F \in \mathscr{M}(J, \pi)$ if and only if π is a complete set of primes in J.

2. Let G be a finitely generated torsion-free group. Suppose that there is a normal abelian subgroup A such that G/A is nilpotent. If π is any infinite set of primes, prove that $\bigcap_{p \in \pi} A^p = 1$.

3. Let G be a finite extension of a polycyclic group and let J be a principal ideal domain. If M is a finitely generated JG-module, show that $M \in \mathscr{M}(J, \pi)$ where π is a finite set of primes in J.

4. If G is a finite extension of a finitely generated nilpotent group, prove that a simple $\mathbb{Z}G$-module is finite.

*5. (P. Hall). Let G be a finitely generated group which is a finite extension of a metanilpotent group. Prove that all principal factors of G are finite and all maximal subgroups of G have finite index. [*Hint*: Use Exercise 15.4.4.]

6. (P. Hall). The main theorems of this section do not hold for finitely generated soluble groups of derived length 3. Use the following construction. Let V be a rational vector space with a basis $\{v_i | i \in \mathbb{Z}\}$ and let the set of all primes be ordered as $\{p_i | i \in \mathbb{Z}\}$ with $p_i \neq p_j$ if $i \neq j$. Define ξ and η in $\mathrm{GL}(V)$ as follows:

$$v_i\xi = v_{i+1} \qquad \text{and} \qquad v_i\eta = p_i v_i.$$

Establish the following statements.
(a) $H = \langle \xi, \eta \rangle$ is isomorphic with the standard wreath product $\mathbb{Z} \wr \mathbb{Z}$, a finitely generated metabelian group.
(b) V is a simple $\mathbb{Z}H$-module.
(c) $G = H \ltimes V$ is a finitely generated soluble group with derived length 3 satisfying max-n.
(d) G is not residually finite, and it has an infinite principal factor and a maximal subgroup of infinite index.

15.5. Finitely Generated Soluble Groups and Their Frattini Subgroups

In Chapter 5 several characterizations of the Fitting subgroup were given, for example in terms of the centralizers of the principal factors (see 5.2.9 and 5.2.15). Similar characterizations were discovered by P. Hall to hold for certain finitely generated soluble groups.

15.5.1 (P. Hall). *Let G be a finitely generated metanilpotent group. Then the following subgroups of G coincide and are nilpotent.*

(i) *The Fitting subgroup.*
(ii) *The Hirsch–Plotkin radical.*

(iii) *The subgroup* FFrat G *defined by the equation*

$$\text{FFrat } G/\text{Frat } G = \text{Fit}(G/\text{Frat } G).$$

(iv) *The intersection of the centralizers of the principal factors of* G.

One consequence of this theorem is that Frat $G \leq$ Fit G; thus *the Frattini subgroup of* G *is nilpotent.*

Behind 15.5.1 stands another version of the Hilbert *Nullstellensatz*, usually referred to as the *Strong Nullstellensatz*. The form of this important theorem which is required here is as follows.

15.5.2. *Let* G *be a finitely generated nilpotent group with integral group ring* R. *Suppose that* M *is a finitely generated* R-*module and* z *a central element of* R *such that* $Mz \leq N$ *for every maximal submodule* N. *Then* $Mz^n = 0$ *for some positive integer* n.

Proof. M is a noetherian module by 15.3.3. Thus we can assume the result to be false for M but true for every proper image of M. Recall that

$$*z = \{a \in M \mid az = 0\};$$

since z is central in R, this is a submodule of M. If $*z \neq 0$, then $Mz^m \leq *z$ for some positive m, which implies that $Mz^{m+1} = 0$. By this contradiction $*z = 0$, so that the R-endomorphism $a \mapsto az$ is injective and $M \simeq^R Mz$.

Let M_1 be an R-module isomorphic with M by means of the assignment $a \mapsto a_1$, $(a \in M, a_1 \in M_1)$. Then $a \mapsto a_1 z$ is surely an injective R-homomorphism from M to M_1 with image $M_1 z$. We may therefore embed M in M_1 as $M_1 z$. By repeated use of this device one obtains a sequence of R-modules $M = M_0, M_1, \ldots$ and embeddings $M_i \to M_{i+1}$ with image $M_{i+1}z$. Let $\overline{M}$ be the direct limit of this sequence of maps and modules. Then, after suitable identifications, we can think of $\overline{M}$ as the union of the chain

$$M = M_0 \leq M_1 \leq \cdots.$$

Since $\overline{M}z \geq M_{i+1}z = M_i$, we have $\overline{M} = \overline{M}z$. Therefore $a \mapsto az$ is an R-automorphism of $\overline{M}$.

Now form the direct product $\overline{G} = G \times T$ where $T = \langle t \rangle$ is an infinite cyclic group. Make $\overline{M}$ into a $\overline{G}$-module by defining at to be az, $(a \in \overline{M})$; this is compatible with the action of G because z is central in R. From $M_i = M_{i+1}z$ it follows that $M_i = Mt^{-i}$. Since $\overline{M}$ is the union of the M_i, we conclude that $\overline{M}$ is finitely generated as a $\mathbb{Z}\overline{G}$-module. Consequently $\overline{M}$ has a maximal $\mathbb{Z}\overline{G}$-submodule, say L. Suppose that L contains M; then L will also contain $Mt^{-i} = M_i$, which gives the contradiction $L = \overline{M}$. Therefore $L \cap M \neq M$.

By 15.4.4 the simple $\mathbb{Z}\overline{G}$-module $\overline{M}/L$ is finite. Thus $M/L \cap M$ is a nontrivial finite abelian group. Now $L \cap M$ is contained in some maximal R-submodule of M, say M^*. By hypothesis $Mz \leq M^*$; thus application of z to

$M/L \cap M$ yields an endomorphism which is not surjective. Since $M/L \cap M$ is finite, this endomorphism cannot be injective either, so there is an a in $M \backslash L$ such that $az \in L \cap M$. Hence $(a + L)z = L$. But this cannot be true since $b \mapsto bz$ is an automorphism of $\bar{M}$ and it induces an automorphism in $\bar{M}/L$. □

***Proof of* 15.5.1.** By hypothesis the finitely generated group G has a nilpotent normal subgroup N such that G/N is nilpotent, and certainly $N \leq \text{Fit } G = F$, say. Since G/N satisfies max, F is the product of *finitely* many normal nilpotent subgroups. Hence F is nilpotent by 5.2.8.

Consider next the Hirsch–Plotkin radical H of G. Of course $F \leq H$; we aim to show that H centralizes every principal factor of G and to achieve this it is sufficient to prove that H centralizes every minimal normal subgroup L of G. This is clear if $H \cap L = 1$, so assume that $L \leq H$. Now L is finite by Exercise 15.4.5, so there is a principal factor of H of the form L/M. Then L/M is central in H because H is locally nilpotent—here we are appealing to 12.1.6. Thus $[L, H] < L$. But $[L, H] \lhd G$, so we obtain $[L, H] = 1$ as required. It follows that $H \leq X$ where X is the intersection of the centralizers of the principal factors of G.

The next step in the proof is to demonstrate that X is nilpotent; for then it will follow that $X \leq F$, and hence that $F = H = X$. If this is not true, X/F is nontrivial and must contain a nontrivial element of the center of G/F, say zF. Consider the $\mathbb{Z}(G/F)$-module $\bar{F} = F/F'$: this is noetherian by 15.3.1. If S is a maximal submodule of $\bar{F}$, then z will centralize $\bar{F}/\bar{S}$ because $z \in X$; in other words $z - 1$ annihilates the module $\bar{F}/\bar{S}$. According to 15.5.2 this implies that some $(z - 1)^n$ annihilates $\bar{F}$, which, translated into the language of group theory, says that $\langle z, F \rangle/F'$ is nilpotent. However if follows from 5.2.10 that $\langle z, F \rangle$ is nilpotent, while $\langle z, F \rangle$ is normal in G because zF was chosen from the center of G/F. Therefore $z \in F$, which is false.

Finally we consider $Y = \text{FFrat } G$. It is clear that $F \leq Y$. All that remains to be done is to show that $Y \leq F$.

In fact we need only do this in the case where N is abelian. For suppose that this has been achieved. By Exercise 12.2.15, we have $N' \leq \text{Frat } G$, so that $\text{Frat}(G/N') = (\text{Frat } G)/N'$ and $\text{FFrat}(G/N') = (\text{FFrat } G)/N'$. Hence Y/N' is nilpotent. Since N is nilpotent, we may deduce from 5.2.10 that Y is nilpotent and $Y \leq F$.

In the remainder of the proof we assume that N is abelian, so that G is residually finite by 15.4.1. Let L be a minimal normal subgroup of G. We need only check that $[Y, L] = 1$. Now L is certainly finite (Exercise 15.4.5). By residual finiteness we can find a $T \lhd G$ such that G/T is finite and $L \cap T = 1$. Obviously $\text{Frat}(G/T) \geq (\text{Frat } G)T/T$, so that $\text{FFrat}(G/T) \geq YT/T$. But $\text{FFrat}(G/T) = \text{Fit}(G/T)$ by Gaschütz's theorem (5.2.15), so $YT/T \leq \text{Fit}(G/T)$. Also $L \simeq^G LT/T$, which implies that LT/T is minimal normal in G/T. We deduce from 5.2.9 that YT/T centralizes LT/T and $[L, Y] \leq L \cap T = 1$. The proof is now complete.

The following useful theorem is a consequence of 15.5.2. It is a generalization of a theorem of Hirsch on polycyclic groups (5.4.18).

15.5.3 (Robinson, Wehrfritz). *Suppose that G is a finitely generated soluble group. If G is not nilpotent, then it has a finite image that is not nilpotent.*

Proof. Presuming the theorem to be false, we choose for G a counterexample of smallest derived length. If A is the smallest nontrivial term of the derived series, then G/A is nilpotent and, of course, A is abelian. Therefore G satisfies max-*n*. By passing to a suitable quotient group we may assume that each proper quotient group of G is nilpotent.

Write $F = \text{Fit } G$. Then F is nilpotent by max-*n*. If $F' \neq 1$, then G/F' is nilpotent, which implies that G is nilpotent. Consequently F is abelian. In addition G/F is nilpotent because F cannot equal 1.

Since $F \neq G$, there is a nontrivial element in the center of G/F, say zF. Using max-*n* we may choose a maximal $\mathbb{Z}(G/F)$-submodule M of F; then F/M is finite. If $M = 1$, the group G is actually polycyclic, in which case the theorem is known to be true (5.4.18). Hence $M \neq 1$ and G/M is nilpotent. Since F/M is minimal normal in G/M, it is central; thus $[F, z] \leq M$. Applying 15.5.2 we deduce that $[F, {}_n z] = 1$ for some $n > 0$. However, this says that $\langle z, F \rangle$ is nilpotent and causes z to lie in F. □

In conclusion we illustrate the use of the last theorem.

15.5.4. *Suppose that G is a group whose Frattini subgroup is finitely generated. Then* Frat G *is nilpotent if and only if it is soluble.*

The proof goes exactly like that of 5.4.19, appeal being made to 15.5.3 at the appropriate point. However, despite 15.5.4, the Frattini subgroup of a finitely generated soluble group may fail to be nilpotent, as examples of P. Hall show ([a78]).

Exercises 15.5

1. (P. Hall). If G is a finitely generated soluble group with nilpotent length $l + 1$, then Frat G has nilpotent length at most l. (The nilpotent length of an infinite soluble group is the length of a shortest series with nilpotent factors.)
2. Prove 15.5.4.
3. A finitely generated soluble group G such that $G' \leq \text{Frat } G$ is nilpotent (see 5.2.16).
4. Is the preceding exercise correct if the group is not finitely generated?
5. (Baer). If G is a finitely generated, nonnilpotent group, prove that G has a quotient group $\bar{G}$ which is not nilpotent but all of whose proper quotient groups are nilpotent.

6. Suppose that G is a finitely generated group which has an ascending normal series each of whose factors is finite or abelian. If G is nonnilpotent, then G has a finite nonnilpotent image. [*Hint*: Use Exercise 15.5.5.]

7. An automorphism α of a group G is said to be *uniform* if the mapping $x \mapsto x^{-1}x^{\alpha}$ is surjective. If G is a finite group, then α is uniform if and only if α is fixed-point-free. Show that this is false for infinite groups.

8. (Robinson, Zappa). Let G be a finitely generated soluble group. If G has a uniform automorphism of prime order, prove that G is a finite nilpotent p'-group. [*Hint*: Use 15.5.3 and 10.5.4.]

9. Prove that 15.5.1 remains true if we allow G to be a *finite extension* of a finitely generated metanilpotent group.

Bibliography

Items marked with an asterisk are in Russian.

Articles

[a1] Asar, A.O., A conjugacy theorem for locally finite groups, *J. London Math. Soc.* (2) **6** (1973), 358–360.

[a2] Auslander, L., On a problem of Philip Hall, *Ann. Math.* (2) **86** (1967), 112–116.

[a3] Ayoub, C., On properties possessed by solvable and nilpotent groups, *J. Austral. Math. Soc.* **9** (1969), 218–227.

[a4] Baer, R., The subgroup of the elements of finite order of an abelian group, *Ann. Math.* **37** (1936), 766–781.

[a5] Baer, R., Nilpotent groups and their generalizations, *Trans. Amer. Math. Soc.* **47** (1940), 393–434.

[a6] Baer, R., Representations of groups as quotient groups, *Trans. Amer. Math. Soc.* **58** (1945), 295–419.

[a7] Baer, R., Finiteness properties of groups, *Duke Math. J.* **15** (1948), 1021–1032.

[a8] Baer, R., Groups with descending chain condition for normal subgroups, *Duke Math. J.* **16**, (1949), 1–22.

[a9] Baer, R., Endlichkeitskriterien für Kommutatorgruppen, *Math. Ann.* **124** (1952), 161–177.

[a10] Baer, R., Nilgruppen, *Math. Z.* **62** (1955), 402–437.

[a11] Baer, R., Classes of finite groups and their properties, *Illinois J. Math.* **1** (1957), 115–187.

[a12] Baer, R., Engelsche Elemente Noetherscher Gruppen, *Math. Ann.* **133** (1957), 256–270.

[a13] Baer, R., Abzählbar erkennbare gruppentheoretische Eigenschaften, *Math. Z.* **79** (1962), 344–363.

[a14] Baer, R., Polyminimaxgruppen, *Math. Ann.* **175** (1968), 1–43.

[a15] Baer, R. and Levi, F., Freie Produkte und ihre Untergruppen, *Compositio Math.* **3** (1936), 391–398.

[a16] Baumslag, G., Automorphism groups of residually finite groups, *J. London Math. Soc.* **38** (1963), 117–118.

[a17] Bender, H., A group theoretic proof of Burnside's $p^a q^b$-theorem, *Math. Z.* **126** (1972), 327–338.

[a18] Birkhoff, G., On the structure of abstract algebras, *Proc. Cambridge Philos. Soc.* **31** (1935), 433–454.

[a19] Burnside, W., On some properties of groups of odd order II, *Proc. London Math. Soc.* **33** (1901), 257–268.

[a20] Burnside, W., On an unsettled question in the theory of discontinuous groups, *Quart. J. Pure Appl. Math.* **33** (1902), 230–238.

[a21] Burnside, W., On groups of order $p^\alpha q^\beta$, *Proc. London Math. Soc.* (2) **1** (1904), 388–392.

[a22] Cameron, P.J., Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), 1–22.

[a23] Čarin, V.S., *A remark on the minimal condition for subgroups, *Dokl. Akad. Nauk. SSSR* **66** (1949), 575–576.

[a24] Čarin, V.S., *On soluble groups of type A_3, *Mat. Sb.* **54** (1961), 489–499.

[a25] Carter, R.W., Splitting properties of soluble groups, *J. London Math. Soc.* **36** (1961), 89–94.

[a26] Carter, R.W., Nilpotent self-normalizing subgroups of soluble groups, *Math. Z.* **75** (1961), 136–139.

[a27] Carter, R.W. and Hawkes, T.O., The $\mathfrak{F}$-normalizers of a finite soluble group, *J. Algebra* **5** (1967), 176–202.

[a28] Černikov, S.N., *Infinite locally soluble groups, *Mat. Sb.* **7** (1940), 35–64.

[a29] Černikov, S.N., *On special *p*-groups, *Mat. Sb.* **27** (1950), 185–200.

[a30] Černikov, S.N., *Infinite groups with finite layers, *Mat. Sb.* **22** (1948), 101–133 = *Amer. Math. Soc. Translations* (1) **56** (1951), 51–102.

[a31] Černikov, S.N., *On groups with finite classes of conjugate elements, *Dokl. Akad. Nauk SSSR* **114** (1957), 1177–1179.

[a32] Černikov, S.N., *On layer-finite groups, *Mat. Sb.* **45** (1958), 415–416.

[a33] Černikov, S.N., *Finiteness conditions in the general theory of groups, *Uspehi Mat. Nauk* **14** (1959), 45–96 = *Amer. Math. Soc. Translations* (2) **84** (1969), 1–67.

[a34] Chevalley, C. Sur certains groupes simples, *Tôhuku Math. J.* (2) **7** (1955), 14–66.

[a35] Clifford, A.H., Representations induced in an invariant subgroup, *Ann. Math.* **38** (1937), 533–550.

[a36] Cooper, C.D.H., Power automorphisms of a group, *Math. Z.* **107** (1968), 335–356.

[a37] Čunihin, S.A., *On theorems of Sylow's type, *Dokl. Akad. Nauk. SSSR* **66** (1949), 165–168.

[a38] Dedekind, R., Über Gruppen, deren sämtliche Teiler Normalteiler sind., *Math. Ann.* **48** (1897), 548–561.

[a39] Dicman, A.P., *On *p*-groups, *Dokl. Akad. Nauk. SSSR* **15** (1937), 71–76.

[a40] Dicman, A.P., Kuroš, A.G. and Uzkov, A.I., Sylowsche Untergruppen von unendlichen Gruppen, *Mat. Sb.* **3** (1938), 178–185.

[a41] Doerk, K., Minimal nicht überauflösbare, endliche Gruppen, *Math. Z.* **91** (1966), 198–205.

[a42] Durban, J.R., Residually central elements in groups, *J. Algebra* **9** (1968), 408–413.

[a43] Dyer, J.L. and Formanek, E., The automorphism group of a free group is complete, *J. London Math. Soc.* (2) **11** (1975), 181–190.

[a44] Eilenberg, S. and MacLane, S., Cohomology theory in abstract groups I, II, *Ann. Math.* (2) **48** (1947), 51–78, 326–341.
[a45] Feit, W., The current situation in the theory of finite simple groups, *Actes Congrès Intern. Math.* (*Nice 1970*), Vol. 1, 55–93.
[a46] Feit, W. and Thompson, J.G., Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.
[a47] Fischer, B., Gaschütz, W., and Hartley, B., Injektoren endlicher auflösbarer Gruppen, *Math. Z.* **102** (1967), 337–339.
[a48] Fitting, H., Beiträge zur Theorie der Gruppen endlicher Ordnung, *Jahresber. Deutsch. Math. Verein* **48** (1938), 77–141.
[a49] Frattini, G., Intorno alla generazione dei gruppi di operazioni, *Rend. Atti. Accad. Lincei* (4) **1** (1885), 281–285, 455–457.
[a50] Frobenius, G., Ueber Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen, *Berliner Berichte* (1898), 501–515.
[a51] Frobenius, G., Über auflösbare Gruppen V, *S.-B. Preuss, Akad. Berlin* (1901). 1324–1329.
[a52] Frobenius, G. and Stickelberger, L., Über Gruppen von vertauschbaren Elementen, *J. Reine Angew. Math.* **86** (1879), 217–262.
[a53] Gallian, J.A., The search for finite simple groups, *Math. Mag.* **49** (1976), 163–180.
[a54] Gaschütz, W., Zur Erweiterungstheorie endlicher Gruppen, *J. Reine Angew. Math.* **190** (1952), 93–107.
[a55] Gaschütz, W., Über die Φ-Untergruppe endlicher Gruppen, *Math. Z.* **58** (1953), 160–170.
[a56] Gaschütz, W., Gruppen, in denen das Normalteilersein transitiv ist, *J. Reine Angew. Math.* **198** (1957), 87–92.
[a57] Gaschütz, W., Zur Theorie der endlichen auflösbaren Gruppen, *Math. Z.* **80** (1963), 300–305.
[a58] Gaschütz, W., Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen, *J. Algebra* **4** (1966), 1–2.
[a59] Golod, E.S., *On nil-algebras and residually finite p-groups, *Izv. Akad Nauk SSSR Ser. Mat.* **28** (1964), 273–276 = *Amer. Math. Soc. Translations* (2) **48** (1965), 103–106.
[a60] Gorčakov, Yu.M., *On locally normal groups, *Mat. Sb.* **67** (1965), 244–254.
[a61] Grigorčuk, R.I., *Burnside's problem on periodic groups, *Funktsional. Anal. i Prilozhen.* **14** (1980), 53–54.
[a62] Gruenberg, K.W., Residual properties of infinite soluble groups, *Proc. London Math. Soc.* (3) **7** (1957), 29–62.
[a63] Gruenberg, K.W., The Engel elements of a soluble group, *Illinois J. Math.* **3** (1959), 151–168.
[a64] Gruenberg, K.W., The upper central series in soluble groups, *Illinois J. Math.* **5** (1961), 436–466.
[a65] Grün, O., Beiträge zur Gruppentheorie I, *J. Reine Angew. Math.* **174** (1935), 1–14.
[a66] Gupta, N.D. and Sidki, S., On the Burnside problem for periodic groups, *Math. Z.* **182** (1983), 385–388.
[a67] Hall, P., A note on soluble groups, *J. London Math. Soc.* **3** (1928), 98–105.
[a68] Hall, P., A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.* (2) **36** (1934), 29–95.
[a69] Hall, P., A characteristic property of soluble groups, *J. London Math. Soc.* **12** (1937), 198–200.
[a70] Hall, P., On the Sylow systems of a soluble group, *Proc. London Math. Soc.* (2), **43** (1937), 316–323.

[a71] Hall, P., On the system normalizers of a soluble group, *Proc. London Math. Soc.* (2) **43** (1937), 507–528.
[a72] Hall, P., Finiteness conditions for soluble groups, *Proc. London Math. Soc.* (3) **4** (1954), 419–436.
[a73] Hall, P., Theorems like Sylow's, *Proc. London Math. Soc.* (3) **6** (1956), 286–304.
[a74] Hall, P., Finite-by-nilpotent groups, *Proc. Cambridge Philos. Soc.* **52** (1956), 611–616.
[a75] Hall, P., Some sufficient conditions for a group to be nilpotent, *Illinois J. Math.* **2** (1958), 787–801.
[a76] Hall, P., Periodic *FC*-groups, *J. London Math. Soc.* **34** (1959), 289–304.
[a77] Hall, P., On the finiteness of certain soluble groups, *Proc. London Math. Soc.* (3) **9** (1959), 595–622.
[a78] Hall, P., The Frattini subgroups of finitely generated groups, *Proc. London Math. Soc.* (3) **11** (1961), 327–352.
[a79] Hall, P., On non-strictly simple groups, *Proc. Cambridge Philos. Soc.* **59** (1963), 531–553.
[a80] Hall, P. and Higman, G., On the *p*-length of *p*-soluble groups and reduction theorems for Burnside's problem, *Proc. London Math. Soc.* (3) **6** (1956), 1–42.
[a81] Hall, P. and Kulatilaka, C.R., A property of locally finite groups, *J. London Math. Soc.* **39** (1964), 235–239.
[a82] Hartley, B., The residual nilpotence of wreath products, *Proc. London Math. Soc.* (3) **20** (1970), 365–392.
[a83] Hartley, B., A note on the normalizer condition, *Proc. Cambridge Philos. Soc.* **74** (1973), 11–15.
[a84] Hawkes, T.O., On formation subgroups of a finite soluble group, *J. London Math. Soc.* **44** (1969), 243–250.
[a85] Head, T.J., Note on the occurrence of direct factors in groups, *Proc. Amer. Math. Soc.* **15** (1964), 193–195.
[a86] Heineken, H., Eine Bemerkung über engelsche Elemente, *Arch. Math. (Basel)* **11** (1960), 321.
[a87] Heineken, H., Engelsche Elemente der Länge drei, *Illinois J. Math.* **5** (1961), 681–707.
[a88] Heineken, H. and Mohamed, I.J., A group with trivial centre satisfying the normalizer condition, *J. Algebra* **10** (1968), 368–376.
[a89] Higman, G., The units of group-rings, *Proc. London Math. Soc.* (2) **46** (1940), 231–248.
[a90] Higman, G., A finitely generated infinite simple group, *J. London Math. Soc.* **26** (1951), 61–64.
[a91] Higman, G., Complementation of abelian normal subgroups, *Publ. Math. Debrecen* **4** (1956), 455–458.
[a92] Higman, G., Subgroups of finitely presented groups, *Proc. Roy. Soc. London Ser.* **A262** (1961), 455–475.
[a93] Higman, G., Neumann, B.H., and Neumann, H., Embedding theorems for groups, *J. London Math. Soc.* **24** (1949), 247–254.
[a94] Hirsch, K.A., On infinite soluble groups I, *Proc. London Math. Soc.* (2) **44** (1938), 53–60.
[a95] Hirsch, K.A., On infinite soluble groups II, *Proc. London Math. Soc.* (2) **44** (1938), 336–344.
[a96] Hirsch, K.A., On infinite soluble groups III, *Proc. London Math. Soc.* (2) **49** (1946), 184–194.
[a97] Hirsch, K.A., On infinite soluble groups IV, *J. London Math. Soc.* **27** (1952), 81–85.

[a98] Hirsch, K.A., On infinite soluble groups V, *J. London Math. Soc.* **29** (1954), 250–251.

[a99] Hirsch, K.A., Über lokal-nilpotente Gruppen, *Math. Z.* **63** (1955), 290–294.

[a100] Hölder, O., Bildung zusammengesetzer Gruppen, *Math. Ann* **46** (1895), 321–422.

[a101] Hopf, H., Über die Bettischen Gruppen, die zu einer beliebigen Gruppe gehören, *Comment. Math. Helv.* **17** (1944/45), 39–79.

[a102] Hulse, J. A., Automorphism towers of polycyclic groups, *J. Algebra* **16** (1970), 347–398.

[a103] Huppert, B., Normalteiler und maximale Untergruppen endlicher Gruppen, *Math. Z.* **60** (1954), 409–434.

[a104] Itô, N., Note on S-groups, *Proc. Japan Acad.* **29** (1953), 149–150.

[a105] Iwasawa, K., Über die endlichen Gruppen und die Verbände ihrer Untergruppen, *J. Univ. Tokyo* **4** (1941), 171–199.

[a106] Iwasawa, K., Einige Sätze über freie Gruppen, *Proc. Imp. Acad. Tokyo* **19** (1943), 272–274.

[a107] Jategaonkar. A.V., Integral group rings of polycyclic-by-finite groups, *J. Pure Appl. Algebra* **4** (1974), 337–343.

[a108] Jordan, C., Recherches sur les substitutions, *J. Math. Pure Appl.* (2) **17** (1872), 351–363.

[a109] Kalužnin, L.A., Über gewisse Beziehungen zwischen einer Gruppe und ihren Automorphismen, *Berlin Math. Tagung* (1953), 164–172.

[a110] Kalužnin, L. and Krasner, M., Produit complet des groupes de permutations et problème d'extension des groupes, *Acta Sci. Math. Szeged.* **13** (1950), 208–230, **14** (1951), 39–66, 69–82.

[a111] Kappe, L.-C. and Kappe, W.P., On three-Engel groups, *Bull. Austral. Math. Soc.* **7** (1972), 391–405.

[a112] Kargapolov, M.I., *On a problem of O. Yu Schmidt, *Sibirsk Math. Ž.* **4** (1963), 232–235.

[a113] Kegel, O.H., Produkte nilpotenter Gruppen, *Arch. Math.* (*Basel*) **12** (1961), 90–93.

[a114] Kegel, O.H., Noethersche 2-Gruppen sind endlich, *Monatsh. Math.* **71** (1967), 424–426.

[a115] Kegel, O.H. and Wehrfritz, B.A.F., Strong finiteness conditions in locally finite groups, *Math. Z.* **117** (1970), 309–324.

[a116] Kolchin, E.R., On certain concepts in the theory of algebraic matric groups, *Ann. Math.* (2) **49** (1948), 774–789.

[a117] Kostrikin, A.I., *The Burnside problem, *Izv. Akad. Nauk SSSR Ser. Mat.* **23** (1959), 3–34.

[a118] Krull, W., Über verallgemeinerte endliche Abelsche Gruppen, *Math. Ann.* **23** (1925), 161–196.

[a119] Kulikov, L.Ya, *On the theory of abelian groups of arbitrary cardinality, *Mat. Sb.* **9** (1941), 165–182.

[a120] Kulikov, L.Ya, *On the theory of abelian groups of arbitrary power, *Mat. Sb.* **16** (1945), 129–162.

[a121] Kuroš, A.G., Die Untergruppen der freien Produkte von beliebigen Gruppen, *Math. Ann.* **109** (1934), 647–660.

[a122] Kuroš, A.G. and Černikov, S.N., *Soluble and nilpotent groups, *Uspehi Mat. Nauk* **2** (1947), 18–59 = *Amer. Math. Soc. Translations* **80** (1953).

[a123] Lennox, J.C. and Roseblade, J.E., Centrality in finitely generated soluble groups, *J. Algebra* **16** (1970), 399–435.

[a124] Levi, F.W., Groups in which the commutator operation satisfies certain algebraic conditions, *J. Indian Math. Soc.* **6** (1942), 87–97.

[a125] Levi, F.W. and van der Waerden, B.L., Über eine besondere Klasse von Gruppen, *Abh. Math. Sem. Univ. Hamburg* **9** (1932), 154–158.

[a126] Lyndon, R.C., The cohomology theory of group extensions, *Duke Math. J.* **15** (1948), 271–292.

[a127] MacLane, S., Cohomology theory in abstract groups III, *Ann. Math.* (2) **50** (1949), 736–761.

[a128] MacLane, S., A proof of the subgroup theorem for free products, *Mathematika* **5** (1958), 13–19.

[a129] Magnus, W., Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring, *Math. Ann.* **111** (1935), 259–280.

[a130] Magnus, W., Über freie Faktorgruppen und freie Untergruppen gegebener Gruppen, *Monatsh. Math. Phys.* **47** (1939), 307–313.

[a131] Mal'cev, A.I., *On the faithful representation of infinite groups by matrices, *Mat. Sb.* **8** (1940), 405–422 = *Amer. Math. Soc. Translations* (2) **45** (1965), 1–18.

[a132] Mal'cev, A.I., *On a general method of obtaining local theorems in group theory, *Ivanov. Gos. Ped. Inst. Učen. Zap.* **1** (1941), 3–9.

[a133] Mal'cev, A.I., *Generalized nilpotent algebras and their adjoint groups, *Mat. Sb.* **25** (1949), 347–366 = *Amer. Math. Soc. Translations* (2) **69** (1968), 1–21.

[a134] Mal'cev, A.I., *On certain classes of infinite soluble groups, *Math. Sb.* **28** (1951), 567–588 = *Amer. Math. Soc. Translations* (2) **2** (1956), 1–21.

[a135] Mal'cev, A.I., *Homomorphisms of finite groups, *Ivanov Gos. Ped. Inst. Učen. Zap.* **18** (1958), 49–60.

[a136] Mathieu, E., Mémoire sur l'étude des fonctions de plusieur quantités, *J. Math. Pures Appl.* (2) **6** (1861), 241–323.

[a137] Mathieu, E.. Sur la fonction cinq fois transitive de 24 quantités, *J. Math. Pures Appl.* (2) **18** (1873), 25–46.

[a138] McLain, D.H., A characteristically-simple group, *Proc. Cambridge Philos. Soc.* **50** (1954), 641–642.

[a139] McLain, D.H., On locally nilpotent groups, *Proc. Cambridge Philos. Soc.* **52** (1956), 5–11.

[a140] McLain, D.H., Finiteness conditions in locally soluble groups, *J. London Math. Soc.* **34** (1959), 101–107.

[a141] Meldrum, J.D.P., On the Heineken–Mohamed groups, *J. Algebra* **27** (1973), 437–444.

[a142] Neumann, B.H., Identical relations in groups I, *Math. Ann.* **114** (1937), 506–525.

[a143] Neumann, B.H., Groups with finite classes of conjugate elements, *Proc. London Math. Soc.* (3) **1** (1951), 178–187.

[a144] Neumann, B.H., An essay on free products of groups with amalgamations, *Philos. Trans. Roy. Soc. A* **246** (1954), 503–554.

[a145] Neumann, B.H. and Neumann, H., Embedding theorems for groups, *J. London Math. Soc.* **34** (1959), 465–479.

[a146] Newman, M.F., On a class of nilpotent groups, *Proc. London Math. Soc.* (3) **10** (1960), 365–375.

[a147] Newman, M.F., The soluble length of soluble linear groups, *Math. Z.* **126** (1972), 59–70.

[a148] Newman, M.F., Problems, in "Burnside Groups", Lecture Notes in Math. Vol. 806, Springer-Verlag, Berlin (1980), 249–254.

[a149] Nielsen, J., Om Regning med ikke kommutative Faktoren og dens Anvendelse i Gruppeteorien, *Mat. Tidssk. B* (1921), 77–94.

[a150] Novikov, P.S. and Adjan, S.I., *Infinite periodic groups, *Izv. Akad. Nauk SSSR Ser. Mat.* **32** (1968), 212–244, 251–524, 709–731 = *Math. USSR–Izv* **2** (1968) 209–236, 241–479, 665–685.

[a151] Novikov, P.S. and Adjan, S.I., *Commutative subgroups and the conjugacy problem in free periodic groups of odd order, *Izv. Akad. Nauk SSSR Ser. Mat.* **32** (1968), 1176–1190 = *Math. USSR–Izv.* **2** (1968), 1131–1144.

[a152] Ol'sanskii, A.Yu, *An infinite group with subgroups of prime orders, *Izv. Akad. Nauk. SSSR Ser. Mat.* **44** (1980), 309–321.

[a153] Peng, T.A., Engel elements of groups with maximal condition on abelian subgroups. *Nanta Math.* **1** (1966), 23–28.

[a154] Peng, T.A., Finite groups with pro-normal subgroups, *Proc. Amer. Math. Soc.* **20** (1969), 232–234.

[a155] Phillips, R.E. and Roseblade, J.E., A residually central group that is not a *Z*-group, *Michigan Math. J.* **25** (1978), 233–234.

[a156] Plotkin, B.I., *On some criteria of locally nilpotent groups, *Uspehi Mat. Nauk* **9** (1954), 181–186 = *Amer. Math. Soc. Translations* (2) **17** (1961), 1–7.

[a157] Plotkin, B.I., *Radical groups, *Mat. Sb.* **37** (1955), 507–526 = *Amer. Math. Soc. Translations* (2) **17** (1961), 9–28.

[a158] Plotkin, B.I., *Generalized soluble and nilpotent groups, *Uspehi Mat. Nauk* **13** (1958), 89–172 = *Amer. Math. Soc. Translations* (2) **17** (1961), 29–115.

[a159] Polovickiĭ, Ya.D., *Layer-extremal groups, *Mat. Sb.* **56** (1962), 95–106.

[a160] Prüfer, H., Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen, *Math. Z.* **17** (1923), 35–61.

[a161] Rae, A. and Roseblade, J.E., Automorphism towers of extremal groups, *Math. Z.* **117** (1970), 70–75.

[a162] Razmyslov, Yu.P., The Hall–Higman Problem, *Izv. Akad. Nauk. SSSR Ser. Mat.* **42** (1978), 833–867.

[a163] Remak, R., Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren, *J. Reine Angew. Math.* **139** (1911), 293–308.

[a164] Remak, R., Über minimale invariante Untergruppen in der Theorie der endlichen Gruppen, *J. Reine Angew. Math.* **162** (1930), 1–16.

[a165] Remak, R., Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte, *J. Reine Angew. Math.* **163** (1930), 1–44.

[a166] Robinson, D.J.S., Groups in which normality is a transitive relation, *Proc. Cambridge Philos. Soc.* **60** (1964), 21–38.

[a167] Robinson, D.J.S., Joins of subnormal subgroups, *Illinois J. Math.* **9** (1965), 144–168.

[a168] Robinson, D.J.S., On the theory of subnormal subgroups, *Math. Z.* **89** (1965), 30–51.

[a169] Robinson, D.J.S., A note on finite groups in which normality is transitive, *Proc. Amer. Math. Soc.* **19** (1968), 933–937.

[a170] Robinson, D.J.S., Hypercentral ideals, noetherian modules and a theorem of Stroud, *J. Algebra* **32** (1974), 234–239.

[a171] Robinson, D.J.S., A new treatment of soluble groups with finiteness conditions on their abelian subgroups, *Bull. London Math. Soc.* **8** (1976), 113–129.

[a172] Robinson, D.J.S., Recent results on finite complete groups, in *Algebra Carbondale* 1980, Lecture Notes in Math. Vol. 848, Springer-Verlag, Berlin (1981), 178–185.

[a173] Roseblade, J.E., On certain subnormal coalition classes, *J. Algebra* **1** (1964), 132–138.

[a174] Roseblade, J.E, On groups in which every subgroup is subnormal, *J. Algebra* **2** (1965), 402–412.

[a175] Roseblade, J.E., The permutability of orthogonal subnormal subgroups, *Math. Z.* **90** (1965), 365–372.

[a176] Roseblade, J.E., A note on subnormal coalition classes, *Math. Z.* **90** (1965), 373–375.
[a177] Roseblade, J.E., The derived series of a join of subnormal subgroups, *Math. Z.* **117** (1970), 57–69.
[a178] Roseblade, J.E., The integral group rings of hypercentral groups, *Bull. London Math. Soc.* **3** (1971), 351–355.
[a179] Roseblade. J.E., Group rings of polycyclic groups, *J. Pure Appl. Algebra* **3** (1973), 307–321.
[a180] Roseblade, J.E., Applications of the Artin–Rees lemma to group rings, *Symposia Math.* **17** (1976), 471–478.
[a181] Roseblade, J.E. and Stonehewer, S.E., Subjunctive and locally coalescent classes of groups, *J. Algebra* **8** (1968), 423–435.
[a182] Sanov, I.N., *Solution of Burnside's problem for exponent 4, *Leningrad State Univ. Annals* (*Učen. Zap.*) *Mat. Ser.* **10** (1940), 166–170.
[a183] Schenkman, E., The splitting of certain solvable groups, *Proc. Amer. Math. Soc.* **6** (1955), 286–290.
[a184] Schenkman, E., On the norm of a group, *Illinois J. Math.* **4** (1960), 150–152.
[a185] Schmid, P., Every saturated formation is a local formation, *J. Algebra* **51** (1978), 144–148.
[a186] Schmidt, O.J., Sur les produits directs, *Bull. Soc. Math. France* **41** (1913), 161–164.
[a187] Schmidt, O.J., Über Gruppen, deren sämtliche Teiler spezielle Gruppen sind, *Rec. Math. Moscow* **31** (1924), 366–372.
[a188] Schmidt, O.J., *Infinite soluble groups, *Mat. Sb.* **17** (1945), 145–162.
[a189] Schmidt, O.J., *The local finiteness of a class of periodic groups, *Ivbr. Trudi* (1959), 298–300, German translation Math. *Forschungsberichte Bd.* **20** (1973), 79–81.
[a190] Schreier, O., Über die Erweiterung von Gruppen I, *Monatsh. Math. Phys.* **34** (1926), 165–180.
[a191] Schreier, O., Über die Erweiterung von Gruppen II, *Abh. Math. Sem. Univ. Hamburg* **4** (1926), 321–346.
[a192] Schreier, O., Die Untergruppen der freien Gruppen, *Abh. Math. Sem. Univ. Hamburg* **5** (1927), 161–183.
[a193] Schur, I., Neuer Beweis eines Satzes über endliche Gruppen, *S.-B. Preuss Akad. Berlin* (1902), 1013–1019.
[a194] Schur, I., Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. Reine Angew. Math.* **127** (1904), 20–50.
[a195] Schur, I., Untersuchungen über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. Regine Angew. Math.* **132** (1907), 85–137.
[a196] Seksenbaev, K., *On the theory of polycyclic groups. *Algebra i Logika* **4** (1965), 79–83.
[a197] Šmelkin, A.L., *Polycylic groups, *Sibirsk. Mat. Ž.* **9** (1968), 234–235 = *Siberian Math. J.* **9** (1968), 178.
[a198] Specker, E., Additive Gruppen von Folgen ganzer Zahlen, *Portugal. Math.* **9** (1950), 131–140.
[a199] Stewart, A.G.R., On the class of certain nilpotent groups, *Proc. Roy. Soc. London Ser. A* **292** (1966), 374–379.
[a200] Stonehewer, S.E., The join of finitely many subnormal subgroups, *Bull. London Math. Soc.* **2** (1970), 77–82.
[a201] Stonehewer, S.E., Permutable subgroups of infinite groups, *Math. Z.* **125** (1972), 1–16.
[a202] Strebel, R., Finitely presented soluble groups, in *Group Theory*, Essays for Philip Hall, Cambridge University Press, Cambridge (1984).

[a203] Sunkov, V.P., *On locally finite groups with a minimality condition for abelian subgroups, *Algebra i Logika* **9** (1970), 579–615 = *Algebra and Logic* **9** (1970), 350–370.

[a204] Šunkov, V.P., *Locally finite groups of finite rank, *Algebra i Logika* **10** (1971), 199–225 = *Algebra and Logic* **10** (1971), 127–142.

[a205] Swan, R.G., Representations of polycyclic groups, *Proc. Amer. Math. Soc.* **18** (1967), 573–574.

[a206] Sylow, L., Théorèmes sur les groupes de substitutions, *Math. Ann.* **5** (1872), 584–594.

[a207] Taunt, D., On *A*-groups, *Proc. Cambridge Philos. Soc.* **45** (1949), 24–42.

[a208] Thompson, J.G., Finite groups with fixed-point-free automorphisms of prime order, *Proc. Nat. Acad. Sci. U.S.A.* **45** (1959), 578–581.

[a209] Thompson, J.G., Normal *p*-complements for finite groups, *J. Algebra* **1** (1964), 43–46.

[a210] Ulm, H, Zur Theorie der abzählbar-unendlichen Abelschen Gruppen, *Math. Ann.* **107** (1933), 774–803.

[a211] Wehrfritz, B.A.F., Frattini subgroups in finitely generated linear groups, *J. London Math. Soc.* **43** (1968), 619–622.

[a212] Weir, A.J., The Reidemeister–Schreier and Kuroš Subgroup Theorems, *Mathematika* **3** (1956), 47–55.

[a213] Wiegold, J., Groups with boundedly finite classes of conjugate elements, *Proc. Roy. Soc. London Ser. A* **238** (1957), 389–401.

[a214] Wielandt, H., Eine Kennzeichnung der direkten Produkte von *p*-Gruppen, *Math. Z.* **41** (1936), 281–282.

[a215] Wielandt, H., Eine Verallgemeinerung der invarianten Untergruppen, *Math. Z.* **45** (1939), 209–244.

[a216] Wielandt, H., Zum Satz von Sylow, *Math. Z.* **60** (1954), 407–408.

[a217] Wielandt, H., Vertauschbare nachinvariante Untergruppen, *Abh. Math. Sem. Univ. Hamburg* **21** (1957), 55–62.

[a218] Wielandt, H., Über den Normalisator der subnormalen Untergruppen, *Math. Z.* **69** (1958), 463–465.

[a219] Wielandt, H., Über Produkte von nilpotenten Gruppen, *Illinois J. Math.* **2** (1958), 611–618.

[a220] Wielandt, H., Über die Existenz von Normalteilern in endlichen Gruppen, *Math. Nachr.* **18** (1958), 274–280.

[a221] Wielandt, H., Über die Normalstruktur von mehrfach faktorisierbaren Gruppen, *J. Austral. Math. Soc.* **1** (1960), 143–146.

[a222] Wilson, J.S., Some properties of groups inherited by normal subgroups of finite index, *Math. Z.* **114** (1970), 19–21.

[a223] Wilson, J.S., On periodic generalized nilpotent groups, *Bull. London Math. Soc.* **9** (1977), 81–85.

[a224] Witt, E., Die 5-fach transitiven Gruppen von Mathieu, *Abh. Math. Sem. Univ. Hamburg* **12** (1938), 256–264.

[a225] Wong, W.J., On finite groups whose 2-Sylow subgroups have cyclic subgroups of index 2, *J. Austral. Math. Soc.* **4** (1964), 90–112.

[a226] Zaičev, D.I., *On groups which satisfy a weak minimality condition, *Mat. Sb.* **78** (1969), 323–331 = *Math. USSR Sb.* **7** (1969), 315–322.

[a227] Zappa, G., Sui gruppi di Hirsch supersolubili, *Rend. Sem. Mat. Univ. Padova* **12** (1941), 1–11, 62–80.

[a228] Zassenhaus, H., Über endliche Fastkörper, *Abh. Math. Sem. Univ. Hamburg* **11** (1936), 187–220.

[a229] Zassenhaus, H., Beweis eines Satzes über diskrete Gruppen, *Abh. Math. Sem. Univ. Hamburg* **12** (1938), 289–312.

[a230] Zorn, M., Nilpotency of finite groups, *Bull. Amer. Math. Soc.* **42** (1936), 485–486.

Books

[b1] Adjan, S.I., *The Burnside Problem and Identities in Groups*, translated from the Russian by J.C. Lennox and J. Wiegold, Springer-Verlag, Berlin (1978).

[b2] Aschbacher, M., *Finite Group Theory*, Cambridge University Press, New York (1986).

[b3] Atiyah, M.F. and Macdonald, I.G., *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA (1969).

[b4] Baumslag, G., *Lecture Notes on Nilpotent Groups*, American Mathematical Society, Providence, RI (1971).

[b5] Bieri, R., *Homological Dimension of Discrete Groups*, Queen Mary College Mathematics Notes, London (1976).

[b6] Blackburn, N. and Huppert, B., *Finite Groups*, Springer-Verlag, Berlin (1967–82).

[b7] Burnside, W., *Theory of Groups of Finite Order*, 2nd edn., Cambridge University Press, Cambridge (1911) (Dover reprint 1955).

[b8] Cartan, H. and Eilenberg, S., *Homological Algebra*, Princeton University Press, Princeton, NJ (1956).

[b9] Carter, R.W., *Simple Groups of Lie Type*, Wiley–Interscience, New York (1972).

[b10] Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A., *ATLAS of Finite Groups*, Oxford University Press, New York (1985).

[b11] Coxeter, H.S.M., *Introduction to Geometry*, Wiley, New York (1961).

[b12] Coxeter, H.S.M. and Moser, W.O.J., *Generators and Relations for Discrete Groups*, 3rd edn., Springer-Verlag, Berlin (1972).

[b13] Curtis, C.W., and Reiner, I., *Methods of Representation Theory*, Wiley, New York (1981).

[b14] Dickson, L.E., *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig (1901) (Dover reprint 1958).

[b15] Dixon, J.D., *Problems in Group Theory*, Blaisdell, Waltham, MA (1967).

[b16] Dixon, J.D., *The Structure of Linear Groups*, Van Nostrand, London (1971).

[b17] Dixon, J.D. and Puttaswamaiah, B.M., *Modular Representations of Finite Groups*, Academic Press, New York (1977).

[b18] Dixon, M.R., *Sylow Theory, Formations and Fitting Classes in Locally Finite Groups*, World Scientific, Singapore (1994).

[b19] Doerk, K. and Hawkes, T.O., *Finite Soluble Groups*, de Gruyter, Berlin (1992).

[b20] Dornhoff, L., *Group Representation Theory*, 2 vols., Marcel Dekker, New York (1971).

[b21] Epstein, D.B.A., *Word Processing in Groups*, Jones and Bartlet, Boston (1992).

[b22] Feit, W., *Characters of Finite Groups*, Benjamin, New York (1967).

[b23] Fricke, R. and Klein, F., *Vorlesungen über die Theorie der Elliptischen Modulfunktionen*, 2 vols., Teubner, Leipzig (1890–2).

[b24] Fuchs, L., *Abelian Groups*, Pergamon, Oxford, UK (1960).

[b25] Fuchs, L., *Infinite Abelian Groups*, 2 vols., Academic Press, New York (1970–3).

[b26] Gorenstein, D., *Finite Groups*, Harper & Row, New York (1968).

[b27] Gorenstein, D., *Finite Simple Groups*, Plenum Press, New York (1982).

[b28] Griffith, P.A., *Infinite Abelian Group Theory*, University of Chicago Press, Chicago (1970).

[b29] Gruenberg, K.W., *Cohomological Topics in Group Theory*, Lecture Notes in Math., vol. 143, Springer-Verlag, Berlin (1970).

[b30] Gupta, N.D., *Burnside Groups and Related Topics*, University of Manitoba, Winnipeg (1976).
[b31] Hall, M., *The Theory of Groups*, Macmillan, New York (1959).
[b32] Hall, P., *The Edmonton Notes on Nilpotent Groups*, Queen Mary College Mathematics Notes, London (1969).
[b33] Herstein, I.N., *Topics in Ring Theory*, University of Chicago Press, Chicago (1969).
[b34] Hilton, P.J. and Stammbach, U., *A Course in Homological Algebra*, Springer-Verlag, New York (1970).
[b35] Johnson, D.L., *Presentations of Groups*, London Mathematical Society Lecture Notes Series 22, Cambridge (1976).
[b36] Jordan, C., *Traité des Substitutions et des Équations Algébriques*, Gauthier-Villars (1870) (Blanchard reprint 1957).
[b37] Kaplansky, I., *Infinite Abelian Groups*, 2nd edn., University of Michigan Press, Ann Arbor, MI (1969).
[b38] Kargapolov, M.I. and Merzljakov, Ju.I., *Fundamentals of the Theory of Groups*, 2nd edn., translated from the Russian by R.G. Burns, Springer-Verlag, New York (1979).
[b39] Kegel, O.H. and Wehrfritz, B.A.F., *Locally Finite Groups*, North-Holland, Amsterdam (1973).
[b40] Kuroš, A.G., *The Theory of Groups*, 2nd edn., 2 vols., translated from the Russian by K.A. Hirsch, Chelsea, New York (1960).
[b41] Kuroš, A.G., *Gruppentheorie*, 3rd edn., 2 vols., German translation, Akademie-Verlag, Berlin (1972).
[b42] Lennox, J.C. and Stonehewer, S.E., *Subnormal Subgroups*, Oxford University Press, New York (1987).
[b43] Lyndon, R.C. and Schupp, P.E., *Combinatorial Group Theory*, Springer-Verlag, Berlin (1977).
[b44] MacLane, S., *Homology*, Springer-Verlag, Berlin (1967).
[b45] Magnus, W., Karrass, A., and Solitar, D., *Combinatorial Group Theory*, Wiley–Interscience, New York (1966).
[b46] Miller, C.F. III, *On Group Theoretic Decision Problems and Their Classification*, Princeton University Press, Princeton, NJ (1971).
[b47] Neumann, B.H., *Lectures on Topics in the Theory of Infinite Groups*, Tata Institute, Bombay (1960).
[b48] Neumann, H., *Varieties of Groups*, Springer-Verlag, Berlin (1967).
[b49] Passi, I.B.S., *Group Rings and Their Augmentation Ideals*, Lecture Notes in Math., Vol. 715, Springer-Verlag, Berlin (1979).
[b50] Passman, D.S., *Permutation Groups*, Benjamin, New York (1968).
[b51] Passman, D.S., *The Algebraic Structure of Group Rings*, Wiley–Interscience, New York (1977).
[b52] Plotkin, B.I., *Groups of Automorphisms of Algebraic Systems*, translated from the Russian by K.A. Hirsch, Wolters–Noordhoff, Groningen (1972).
[b53] Robinson, D.J.S., *Infinite Soluble and Nilpotent Groups*, Queen Mary College Mathematics Notes, London (1968).
[b54] Robinson, D.J.S., *Finiteness Conditions and Generalized Soluble Groups*, 2 vols., Springer-Verlag, Berlin (1972).
[b55] Robinson, G. de B., *Representation Theory of the Symmetric Group*, Toronto (1961).
[b56] Rose, J.S., *A Course on Group Theory*, Cambridge University Press, Cambridge (1978).
[b57] Rotman, J.J., *An Introduction to the Theory of Groups*, 4th edn., Springer-Verlag, New York (1995).

[b58] Schenkman, E., *Group Theory*, Van Nostrand, Princeton, NJ (1965).
[b59] Schmidt, O.J., *Abstract Theory of Groups*, 2nd edn., translated from the Russian by F. Holling and J.B. Roberts, Freeman, San Francisco (1966).
[b60] Scott, W.R., *Group Theory*, Prentice-Hall, Englewood Cliffs, NJ (1964).
[b61] Segal, D., *Polycyclic Groups*, Cambridge University Press, New York (1983).
[b62] Serre, J.-P., *Linear Representations of Finite Groups*, translated from the French by L.L. Scott, Springer-Verlag, New York (1977).
[b63] Specht, W., *Gruppentheorie*, Springer-Verlag, Berlin (1956).
[b64] Speiser, A., *Die Theorie der Gruppen von Endlicher Ordnung*, 3rd edn., Springer-Verlag, Berlin (1937).
[b65] Steinberg, R., *Lectures on Chevalley Groups*, Yale University Press, New Haven (1967).
[b66] Suprunenko, D.A., *Soluble and Nilpotent Linear Groups*, Translation of Mathematics Monographs, American Mathematical Society (1963).
[b67] Suzuki, M., *Structure of a Group and the Structure of Its Lattice of Subgroups*, Springer-Verlag, Berlin (1956).
[b68] Suzuki, M., *Group Theory*, Springer-Verlag, Berlin (1982).
[b69] Tomkinson, M.J., *FC-Groups*, Pitman, Boston (1984).
[b70] Vaughan-Lee, M., *The Restricted Burnside Problem*, Oxford University Press, New York (1993).
[b71] Wehrfritz, B.A.F., *Infinite Linear Groups*, Springer-Verlag, Berlin (1973).
[b72] Weinstein, M., *Examples of Groups*, Polygonal, Passaic, NJ (1977).
[b73] Weiss, E., *Algebraic Number Theory*, McGraw-Hill, New York (1963).
[b74] Wielandt, H., *Finite Permutation Groups*, translated from the German by R. Bercov, Academic Press, New York (1964).
[b75] Zassenhaus, H., *The Theory of Groups*, 2nd English edn., Chelsea, New York (1958).

Index

Graduate Texts in Mathematics

continued from page ii

119 Rotman. An Introduction to Algebraic Topology.
120 Ziemer. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.
121 Lang. Cyclotomic Fields I and II. Combined 2nd ed.
122 Remmert. Theory of Complex Functions. *Readings in Mathematics*
123 Ebbinghaus/Hermes et al. Numbers. *Readings in Mathematics*
124 Dubrovin/Fomenko/Novikov. Modern Geometry—Methods and Applications. Part III.
125 Berenstein/Gay. Complex Variables: An Introduction.
126 Borel. Linear Algebraic Groups.
127 Massey. A Basic Course in Algebraic Topology.
128 Rauch. Partial Differential Equations.
129 Fulton/Harris. Representation Theory: A First Course. *Readings in Mathematics*
130 Dodson/Poston. Tensor Geometry.
131 Lam. A First Course in Noncommutative Rings.
132 Beardon. Iteration of Rational Functions.
133 Harris. Algebraic Geometry: A First Course.
134 Roman. Coding and Information Theory.
135 Roman. Advanced Linear Algebra.
136 Adkins/Weintraub. Algebra: An Approach via Module Theory.
137 Axler/Bourdon/Ramey. Harmonic Function Theory.
138 Cohen. A Course in Computational Algebraic Number Theory.
139 Bredon. Topology and Geometry.
140 Aubin. Optima and Equilibria. An Introduction to Nonlinear Analysis.
141 Becker/Weispfenning/Kredel. Gröbner Bases. A Computational Approach to Commutative Algebra.
142 Lang. Real and Functional Analysis. 3rd ed.
143 Doob. Measure Theory.
144 Dennis/Farb. Noncommutative Algebra.
145 Vick. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
146 Bridges. Computability: A Mathematical Sketchbook.
147 Rosenberg. Algebraic *K*-Theory and Its Applications.
148 Rotman. An Introduction to the Theory of Groups. 4th ed.
149 Ratcliffe. Foundations of Hyperbolic Manifolds.
150 Eisenbud. Commutative Algebra with a View Toward Algebraic Geometry.
151 Silverman. Advanced Topics in the Arithmetic of Elliptic Curves.
152 Ziegler. Lectures on Polytopes.
153 Fulton. Algebraic Topology: A First Course.
154 Brown/Pearcy. An Introduction to Analysis.
155 Kassel. Quantum Groups.
156 Kechris. Classical Descriptive Set Theory.
157 Malliavin. Integration and Probability.
158 Roman. Field Theory.
159 Conway. Functions of One Complex Variable II.
160 Lang. Differential and Riemannian Manifolds.
161 Borwein/Erdélyi. Polynomials and Polynomial Inequalities.
162 Alperin/Bell. Groups and Representations.
163 Dixon/Mortimer. Permutation Groups.